Larissa Fontes

Larissa M S Fontes - 2025.pdf

TCC-Direito PUC-SP

TCC-Direito PUC-SP

FUNDASP - Fundação São Paulo (PUC SP / UNIFAI)

Detalhes do documento

ID de entrega
trn:oid:::30649:514834508

Data da entrega
18 de out. de 2025, 21:44 BRT

Data de download
19 de out. de 2025, 08:01 BRT

Nome do arquivo
Larissa M S Fontes - 2025.pdf

Tamanho do arquivo
764.9 KB

63 Páginas

21.475 Palavras

123.712 Caracteres

28% Similaridade geral

O total combinado de todas as correspondências, incluindo fontes sobrepostas, para cad...

Principais fontes

24% Fontes da Internet
16% Publicações
19% Trabalhos enviados (documentos de aluno)

Sinalizadores de integridade

0 Sinalizador de integridade para revisão

Nenhuma suspeita de manipulação de texto encontrada.

Os algoritmos do nosso sistema analisam profundamente um documento em busca de inconsistências que o diferenciem de um envio normal. Se notarmos algo estranho, sinalizaremos para você revisar.

Um sinalizador não é necessariamente um indicador de problema. No entanto, recomendamos que você concentre sua atenção nele para fazer uma análise mais aprofundada.

Principais fontes

24% Fontes da Internet
16% Publicações
19% Trabalhos enviados (documentos de aluno)

Principais fontes

As fontes com o maior número de correspondências no envio. Fontes sobrepostas não serão exibidas.

1	Internet	
www.gov.br		2%
2	Internet	
dfj.emnuvens.com.br		<1%
3	Internet	
www.revista.ueg.br		<1%
4	Internet	
pt.scribd.com		<1%
5	Publicação	
Ingo Wolfgang Sarlet. "Proteção da personalidade no ambiente digital: uma análi...		<1%
6	Internet	
www.juridipedia.com		<1%
7	Internet	
repositorio.pucsp.br		<1%
8	Internet	
www.cidp.pt		<1%
9	Internet	
periodicos.ufsc.br		<1%
10	Internet	
acervodigital.ufpr.br		<1%
11	Internet	
atos.cnj.jus.br		<1%

12	Internet	
www.migalhas.com.br		<1%
13	Internet	
repositorio.jesuita.org.br		<1%
14	Internet	
www.teses.usp.br		<1%
15	Internet	
www.mpsp.mp.br		<1%
16	Internet	
dokumen.pub		<1%
17	Internet	
lume.ufrgs.br		<1%
18	Internet	
ariel.pucsp.br		<1%
19	Internet	
bdta.abcd.usp.br		<1%
20	Internet	
repositorio.ufmg.br		<1%
21	Trabalhos enviados	
Fundação Armando Álvares Penteado (FAAP) on 2023-11-06		<1%
22	Internet	
suprema.stf.jus.br		<1%
23	Internet	
ayaeditora.com.br		<1%
24	Internet	
philpapers.org		<1%
25	Internet	
www.informatica-juridica.com		<1%

26 Internet
hdl.handle.net <1%

27 Internet
pdfcoffee.com <1%

28 Trabalhos enviados
AMBRA College -- American College of Brazilian Studies on 2025-09-30 <1%

29 Internet
philarchive.org <1%

30 Internet
repositorio.idp.edu.br <1%

31 Internet
bibliotecatede.uninove.br <1%

32 Trabalhos enviados
Universidade Portucalense on 2024-01-03 <1%

33 Trabalhos enviados
Universidade Presbiteriana Mackenzie, MACKENZIE on 2025-09-26 <1%

34 Internet
irisbh.com.br <1%

35 Internet
itsrio.org <1%

36 Trabalhos enviados
Associacao Paranaense De Cultura on 2024-11-10 <1%

37 Internet
rdai.com.br <1%

38 Internet
www.itm.nrw <1%

39 Internet
revistaeletronica.pge.rj.gov.br <1%

40 Internet
www2.faac.unesp.br <1%

41 Internet
civilistica.com <1%

42 Trabalhos enviados
ufs on 2025-07-10 <1%

43 Internet
www2.senado.leg.br <1%

44 Internet
revistas.unifacs.br <1%

45 Trabalhos enviados
idp on 2025-06-20 <1%

46 Trabalhos enviados
Instituto Brasiliense de Direito Publico on 2021-02-10 <1%

47 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

48 Internet
cetic.br <1%

49 Internet
dialnet.unirioja.es <1%

50 Trabalhos enviados
pucrs on 2025-08-22 <1%

51 Internet
www.repositorio.jesuita.org.br <1%

52 Internet
tede2.pucrs.br <1%

53 Internet
periodicos.univali.br <1%

54 Internet
seer.atitus.edu.br <1%

55 Internet
www.repositorio.ufal.br <1%

56 Publicação
Adriano Cardoso dos Santos. "PRIVACIDAD DE DATOS E INTELIGENCIA ARTIFICIAL... <1%

57 Trabalhos enviados
ESPM - Escola Superior de Propaganda e Marketing on 2025-09-22 <1%

58 Internet
portal.fgv.br <1%

59 Internet
repositorio.ufrn.br <1%

60 Internet
repositorio.ufsc.br <1%

61 Internet
lirias.kuleuven.be <1%

62 Trabalhos enviados
Universidade de Sao Paulo on 2022-05-31 <1%

63 Internet
www.tre-am.jus.br <1%

64 Publicação
Raphael Miziara. "Discriminação algorítmica e direito do trabalho : condições e li... <1%

65 Internet
profmatheus.com <1%

66 Internet
www.passeidireto.com <1%

67 Internet
www.scielo.br <1%

68 Publicação
Daniel de Araujo Dourado, Fernando Mussa Abujamra Aith. "A regulação da inteli... <1%

69 Internet
repositorio2.unb.br <1%

70 Publicação
Rubia Maria Ferrão de Araújo. "Excludentes de responsabilidade civil no contexto... <1%

71 Trabalhos enviados
Universidade Presbiteriana Mackenzie, MACKENZIE on 2025-09-26 <1%

72 Trabalhos enviados
University of Belgrade-Faculty of Political Sciences on 2024-10-08 <1%

73 Internet
repositorio.unaerp.br <1%

74 Publicação
Gabriela Andrade Vitor. "Liberdade de expressão e democracia digital: o novo esp... <1%

75 Trabalhos enviados
Universidade Presbiteriana Mackenzie, MACKENZIE on 2025-10-02 <1%

76 Trabalhos enviados
Universidade de Sao Paulo on 2020-12-13 <1%

77 Publicação
Luiza Gimenez Nonato. "Relações de poder na era da Inteligência Artificial (IA): a ... <1%

78 Internet
www.pinheironeto.com.br <1%

79 Trabalhos enviados
Associacao Paranaense De Cultura on 2025-04-24 <1%

80 Publicação
Rafael Roque Garofano. "Limitação de finalidade no tratamento de dados pessoai... <1%

81 Publicação
Figueiredo, Bárbara Brito. "Criptoativos no Ambito Insolvencial: A Possibilidade e ... <1%

82 Internet
indexlaw.org <1%

83 Internet
revistas.newtonpaiva.br <1%

84 Trabalhos enviados
AMBRA College -- American College of Brazilian Studies on 2025-04-03 <1%

85 Publicação
Daniel de Araujo Dourado. "Regulação da inteligência artificial na saúde", Univer... <1%

86 Internet
br.boell.org <1%

87 Trabalhos enviados
idp on 2025-06-28 <1%

88 Internet
tede2.pucsp.br <1%

89 Trabalhos enviados
Associacao Paranaense De Cultura on 2025-06-01 <1%

90 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

91 Internet
chcadvocacia.adv.br <1%

92 Internet
eur-lex.europa.eu <1%

93 Internet
fliphtml5.com <1%

94 Publicação
Maraisa Rosa Cezarino. "A institucionalização da invisibilidade da identidade de g... <1%

95 Trabalhos enviados
Universidade Portucalense on 2025-02-01 <1%

96 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

97 Trabalhos enviados
autonoma on 2025-06-24 <1%

98 Internet
biblio.ugent.be <1%

99 Internet
sbmfc.org.br <1%

100 Internet
tede.mackenzie.br <1%

101 Publicação
Barbosa, Fernanda. "Características dos Internamentos Hospitalares por COVID-1... <1%

102 Publicação
Guilherme Berti de Campos Guidi. "Proteção de dados pessoais: a composição de ... <1%

103 Trabalhos enviados
Instituto Brasiliense de Direito Publico on 2021-06-07 <1%

104 Publicação
Yelshyna, Aliaksandra. "Segurança e Privacidade no Contexto de Ambientes Inteli... <1%

105 Internet
periodicos.se.df.gov.br <1%

106 Internet
vdocuments.net <1%

107 Internet
www.maxwell.vrac.puc-rio.br <1%

108 Trabalhos enviados
MUST University on 2025-08-28 <1%

109 Publicação
Patz, Stéfani Reimann. "O uso de Tecnologias de Perfilamento no Controle Migrat... <1%

110 Trabalhos enviados
Universidade de Sao Paulo on 2021-06-14 <1%

111 Internet
app.uff.br <1%

112 Internet
experteditora.com.br <1%

113 Internet
gedai.ufpr.br <1%

114 Internet
ibda.com.br <1%

115 Trabalhos enviados
pucrs on 2025-08-03 <1%

116 Internet
repositorio.fdci.edu.br <1%

117 Internet
www.dolcegabbana.com <1%

118 Internet
www.periodicos.unis.edu.br <1%

119 Publicação
"Desafios do Direito frente às novas tecnologias", Editora Cientifica Digital, 2024 <1%

120 Publicação
Ivan Dias da Motta, Tatiana Manna Bellasalma e Silva. "A Proteção de Dados Sens... <1%

121 Trabalhos enviados
idp on 2024-10-07 <1%

122 Internet
mittechreview.com.br <1%

123 Internet
www.machadomeyer.com.br <1%

124 Trabalhos enviados
MUST University on 2025-06-09 <1%

125 Internet
focusingonwildlife.com <1%

126 Internet
pantheon.ufrj.br <1%

127 Trabalhos enviados
pucrs on 2025-07-04 <1%

128 Trabalhos enviados
Universidade do Porto on 2023-05-26 <1%

129 Trabalhos enviados
Unviersidad de Granada on 2024-03-18 <1%

130 Trabalhos enviados
idp on 2025-06-12 <1%

131 Internet
revistaapolice.com.br <1%

132 Internet
www.anamatra.org.br <1%

133 Publicação
Letícia Araújo Alves, Orione Dantas de Medeiros. "DIREITOS FUNDAMENTAIS DIGI... <1%

134 Trabalhos enviados
idp on 2024-10-17 <1%

135 Internet
repositorio.unb.br <1%

136 Internet
tede.pucsp.br <1%

137 Trabalhos enviados
Fundação Armando Álvares Penteado (FAAP) on 2025-03-23 <1%

138 Trabalhos enviados
Instituto Brasiliense de Direito Publico on 2020-12-15 <1%

139 Trabalhos enviados
Universidade Presbiteriana Mackenzie, MACKENZIE on 2025-06-05 <1%

140 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

141 Internet
vlex.com.br <1%

142 Internet
web.trf3.jus.br <1%

143 Internet
www.brunomiragem.com.br <1%

144 Internet
www.publicacoesacademicas.uniceub.br <1%

145 Trabalhos enviados
ESPM - Escola Superior de Propaganda e Marketing on 2025-10-17 <1%

146 Publicação
João Vitor Marques Fernandes. "O regime jurídico da responsabilidade civil na Lei... <1%

147 Trabalhos enviados
Universidad Estadual Paulista on 2025-06-18 <1%

148 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

149 Internet
www.fmp.edu.br <1%

150 Internet
www.locus.ufv.br <1%

151 Internet
www.notredame.org.br <1%

152 Internet
www.researchgate.net <1%

153 Publicação
Camara, Geysa. "Do Reconhecimento Facial Estudo Exploratório e Análise Compar... <1%

154 Publicação
Camila Salgueiro da Purificação Marques, Cinthia Obladen de Almendra Freitas. "... <1%

155 Publicação
Danilo Vieira Vilela, Thalles Ricardo Alciati Valim, Vanessa De Castro Rosa, Viniciu... <1%

156 Trabalhos enviados
MUST University on 2025-08-13 <1%

157 Trabalhos enviados
MUST University on 2025-09-11 <1%

158 Publicação
Milton Yasuo Fujimoto. "Segredo de negócios, proteção de dados pessoais e inteli... <1%

159 Publicação
Renato Leite Monteiro. "Desafios para a efetivação do direito à explicação na Lei ... <1%

160 Trabalhos enviados
Universidade Nova De Lisboa on 2025-06-12 <1%

161 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

162 Trabalhos enviados
Universidade de Sao Paulo on 2022-06-21 <1%

163 Trabalhos enviados
University of Malaya on 2010-04-26 <1%

164 Internet
books.openedition.org <1%

165 Internet
danielvidor.jusbrasil.com.br <1%

166 Internet
edemocracia.camara.leg.br <1%

167 Trabalhos enviados
pucrs on 2025-06-23 <1%

168 Internet
repositorio.ufob.edu.br <1%

169 Internet
sistemas.uft.edu.br <1%

170 Trabalhos enviados
ufgd on 2025-08-18 <1%

171 Internet
www.coursehero.com <1%

172 Internet
www.rbc.org.br <1%

173 Trabalhos enviados
(school name not available) on 2024-12-05 <1%

174 Trabalhos enviados
AMBRA College -- American College of Brazilian Studies on 2025-10-13 <1%

175 Trabalhos enviados
Associacao Paranaense De Cultura on 2025-05-17 <1%

176 Trabalhos enviados
Associatie K.U.Leuven on 2012-08-21 <1%

177 Publicação
Carvalho, Stephanie Goldstein Costa. "Proteção de Dados Sensíveis do Trabalhad... <1%

178 Trabalhos enviados
Dublin City University on 2011-08-28 <1%

179 Trabalhos enviados
IPS Instituto Politécnico de Setubal on 2023-12-29 <1%

180 Publicação
Igor Venceslau. "Espaço geográfico e economia digital: usos do território brasileir... <1%

181 Trabalhos enviados
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa on 2021-12-27 <1%

182 Publicação
Ludmilla Rocha Cunha Ribeiro. "Inteligência artificial e decisão administrativa: int... <1%

183 Publicação
Primaz, Luís Eduardo. "Colonialismo Digital: As Marcas da Colonialidade no Uso e ... <1%

184 Publicação
Rafael Lucas Borba, Iuri Emmanuel de Paula Ferreira, Paulo Henrique Bertucci Ra... <1%

185 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

186 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

187 Internet
bdm.unb.br <1%

188 Publicação
dos Santos Naves, Gabriela Gomes. "A Morte é Mesmo o fim de Tudo? Herança Di... <1%

189 Internet
dspace.mackenzie.br <1%

190 Internet
ebin.pub <1%

191 Internet
economyandsociety.in.ua <1%

192 Trabalhos enviados
ifsp on 2025-01-17 <1%

193 Internet
journalppc.com <1%

194 Internet
publicador.sestsenat.org.br <1%

195 Internet
repositorio.aee.edu.br <1%

196 Internet
repositorio.animaeducacao.com.br <1%

197 Internet
revista.internetlab.org.br <1%

198 Internet
static.juremy.com <1%

199 Trabalhos enviados
ufsm on 2025-07-17 <1%

200 Internet
www.advogado.adv.br <1%

201 Internet
www.cpjm.uerj.br <1%

202 Internet
www.revista.agulha.nom.br <1%

203 Publicação
Farias, James Magno Araújo. "Direito, Tecnologia e Justiça Digital: O Uso de Ferra... <1%

204 Publicação
Mendes, Laura Schertel(Pinto, Cristiano Otávio Paixão Araújo). "Transparência e p... <1%

205 Publicação
Rodrigo Amaral Paula de Méo. "Inteligência artificial : reflexos na responsabilida... <1%

206 Trabalhos enviados
Universidade de Fortaleza -- Fundação Edson Queiroz / Foundation Edson Queiroz... <1%

207 Publicação
Veridiana Alimonti. "Algoritmos e autodeterminação: uma contribuição a partir d... <1%

208 Publicação
Vitória Bittar Teixeira. "Análise dos sistemas de pontuação de crédito das fintech... <1%

209 Internet
repositorio.ufpb.br <1%

210 Trabalhos enviados
Associacao Paranaense De Cultura on 2024-11-18 <1%

211 Publicação
Borges, Gabriela Coelho Mesquita Teixeira. "Violence and Agency in the Lives of R... <1%

212 Trabalhos enviados
Instituto Brasiliense de Direito Publico on 2020-11-16 <1%

213 Publicação
Letícia Ferrão Zapolla. "A regulação da inteligência artificial sob a perspectiva do ... <1%

214 Publicação
Maria Eugênia Geve de Moraes Lacerda. "Auditorias antidiscriminatórias: diretriz... <1%

215 Publicação
Pes, Joao Helio Ferreira. "A Fundamentalidade Do Direito De Acesso a agua potav... <1%

216 Publicação
Renata Capriolli Zocatelli Queiroz. "A proteção de dados pessoais: a LGPD e a disci... <1%

217 Trabalhos enviados
Universidade de Sao Paulo on 2020-12-09 <1%

218 Trabalhos enviados
Universidade de Sao Paulo on 2023-04-10 <1%

219 Trabalhos enviados
autonoma on 2024-09-10 <1%

220 Publicação
de FrançaMenezes, Tatiane Cardoso Gonçalves. "As Principais Implicações do Reg... <1%

221 Publicação
de Lacerda Silva, Weder. "O Regime Jusfundamental da Proteção de Dados Pesso... <1%

222 Trabalhos enviados

idp on 2024-07-24 <1%

223 Trabalhos enviados

idp on 2024-12-16 <1%

224 Trabalhos enviados

idp on 2025-07-02 <1%

225 Internet

www.portaldeperiodicos.idp.edu.br <1%

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
FACULDADE DE DIREITO

LARISSA MARIA DA SILVA FONTES

A ILUSÃO DA ANONIMIZAÇÃO E OS RISCOS DE DISCRIMINAÇÃO: DADOS SENSÍVEIS E O USO DE IA SOB A PERSPECTIVA DA LGPD

TRABALHO DE CONCLUSÃO DE CURSO

SÃO PAULO
2025

LARISSA MARIA DA SILVA FONTES

A ILUSÃO DA ANONIMIZAÇÃO E OS RISCOS DE DISCRIMINAÇÃO: DADOS SENSÍVEIS E O USO DE IA SOB A PERSPECTIVA DA LGPD

Trabalho de conclusão do curso de Direito, apresentado à Pontifícia Universidade Católica de São Paulo, como requisito parcial para **bacharelado em Direito**, realizado sob a orientação do Prof. Dr. **Vitor Morais de Andrade**.

SÃO PAULO

2025

Sistemas de Bibliotecas da Pontifícia Universidade Católica de São Paulo -
Ficha Catalográfica com dados fornecidos pelo autor

F683a

Fontes, Larissa Maria da Silva
A ILUSÃO DA ANONIMIZAÇÃO E OS RISCOS DE DISCRIMINAÇÃO: DADOS SENSÍVEIS E O USO DE IA SOB A PERSPECTIVA DA LGPD. / Larissa Maria da Silva Fontes ; . -- São Paulo: [s.n.], 2025.
p. ; cm.

Orientador: Vitor Morais de Andrade.
Trabalho de Conclusão de Curso (Graduação) -- Pontifícia Universidade Católica de São Paulo, Graduação em Direito, 2025.

1. Lei Geral de Proteção de Dados. 2. Inteligência Artificial. 3. Anonimização. 4. Discriminação. I. , . II. Andrade, Vitor Morais de. III. Pontifícia Universidade Católica de São Paulo,Trabalho de Conclusão de Curso para Graduação em Direito. IV. Título.

CDD

Banca Examinadora

_____

_____

_____

_____

_____

AGRADECIMENTOS

É com profunda gratidão que registro meus sinceros agradecimentos a todos que foram fundamentais durante minha trajetória acadêmica, em especial ao meu marido Diogo Felipe Alves Fontes, pelo incentivo aos meus estudos desde o cursinho preparatório para a Graduação, por ter aceitado viver essa experiencia comigo quando nos casamos em dezembro de 2021, em meio a pandemia da Covid-19 e no primeiro ano da Graduação, e por ter sido meu ponto de apoio emocional nos momentos mais difíceis dessa jornada.

À minha família e a família do meu marido, pela dedicação, incentivo e compreensão incondicionais, e por sustentarem, com afeto, cada etapa deste percurso. Graças ao apoio emocional de cada um de vocês, foi possível chegar até o final desse curso. Aos meus pais Josefa Maria da Silva e José Antônio da Silva que mesmo possuindo o fundamental incompleto, me ensinaram muito sobre a vida como ela é e a importância trabalho braçal.

Aos professores da Faculdade de Direito da PUC-SP que contribuíram com a minha trajetória acadêmica e profissional, em especial ao meu orientador Prof. Dr. Vitor Morais de Andrade, pelo rigor, pela escuta generosa e pelos ensinamentos transmitidos ao longo desses anos como aluna discente.

Ao Centro Acadêmico 22 de Agosto – Gestão Alvorecer, pelo ambiente colaborativo e pelas oportunidades de crescimento pessoal e institucional, que tanto enriqueceram minha formação. Deixo meu eterno agradecimento aos fundadores e membros ativos: João Brandão, Luiza Martins, Carlos Rodrigues, Carolina Calanca, Leonardo Carvalho, Ana Júlia Carmona, Lais Hera, Henrique Joia, Henrique Lascani e tantos outros, que promoveram com honras as três edições da viagem acadêmica a Brasília para os alunos pagantes e bolsista do curso de Direito.

Aos colegas de profissão, colegas da faculdade e amigos, pela troca constante, pelo apoio mútuo e pela companhia valiosa, que tornam cada conquista mais significativa, especialmente a Dra. Ilaria Lorenza Margherita Sarti, a Dra. Suzana Catta Preta, a Dra. Leticia Sugano, ao Dr. Matheus Colacino, ao Dr. Leonardo Próspero Ortiz e ao Dr. Marco Aurélio de Almeida Alves, pelo incentivo, pela inspiração como profissionais, pelas inúmeras cobranças construtivas e pelo apoio aos estudos acadêmicos e profissionais.

Por fim, agradeço a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho. Dedico este resultado a cada pessoa que acreditou em mim e possibilitou que esta etapa fosse concluída com dedicação, ética e respeito.

"Considerai vossa origem,
pois não fostes feito
para viver como brutos,
mas para ir atrás de virtudes e
de conhecimento."

– Dante Alighieri

RESUMO

A presente pesquisa encontra-se consubstanciada em uma análise jurídica rigorosa acerca da utilização de dados sensíveis por sistemas de inteligência artificial (IA). O tema, premente relevante no contexto do Direito Digital contemporâneo, aborda sobre a expansão tecnológica e da necessidade de aferir a adaptabilidade da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD). O problema fulcral que impulsiona esta investigação pode ser formulado nos seguintes termos: em que medida a anonimização prevista na LGPD é eficaz para proteger dados sensíveis contra discriminação em sistemas de inteligência artificial, e quais adaptações jurídicas e tecnológicas são necessárias para mitigar esses riscos?. Dito isso, a principal hipótese que permeia o trabalho é a de que a anonimização, conforme delineada na LGPD, não possui suficiência para eliminar os riscos de discriminação que acompanham o uso de dados sensíveis por algoritmos de inteligência artificial. Isso se deve, data vênia, à latente possibilidade de reidentificação dos dados previamente anonimizados e à manifesta presença de vieses algorítmicos nos sistemas de IA, os quais podem gerar discriminações não integralmente mitigadas pelas disposições legais vigentes. Outrossim, aventa-se a hipótese de que a ausência de fiscalização efetiva e de regulamentações específicas para o emprego da IA em conjunto com dados sensíveis contribui, de maneira inequívoca, para a perpetuação dessas vulnerabilidades no ordenamento jurídico brasileiro, que reside na urgência e no caráter exponencial do uso da IA em setores vitais, tais como saúde, educação e mercado de trabalho, onde decisões automatizadas impactam diretamente direitos fundamentais, sobretudo o direito à igualdade e à não discriminação. O estudo buscará, assim, contribuir para a compreensão crítica das lacunas da legislação e sugerir soluções que fortaleçam a proteção contra discriminações algorítmicas. Por derradeiro, considera-se que a proposição de soluções técnicas e jurídicas poderá mitigar os riscos de discriminação, promovendo uma maior compatibilidade entre a LGPD e as práticas tecnológicas contemporâneas.

Palavras chave: Direito Digital, Proteção de Dados, Anonimização, LGPD, Inteligência Artificial.

ABSTRACT

This research is based on a rigorous legal analysis of the use of sensitive data by artificial intelligence (AI) systems. The topic, which is highly relevant in the context of contemporary digital law, addresses technological expansion and the need to assess the adaptability of the General Data Protection Law (Law No. 13,709/2018 – LGPD). The central problem driving this investigation can be formulated as follows: to what extent is the anonymization provided for in the LGPD effective in protecting sensitive data against discrimination in artificial intelligence systems, and what legal and technological adaptations are necessary to mitigate these risks? That said, the main hypothesis underlying this work is that anonymization, as outlined in the LGPD, is not sufficient to eliminate the risks of discrimination that accompany the use of sensitive data by artificial intelligence algorithms. This is due, with all due respect, to the latent possibility of re-identification of previously anonymized data and the manifest presence of algorithmic biases in AI systems, which can generate discrimination that is not fully mitigated by current legal provisions. Furthermore, there is a hypothesis that the absence of effective oversight and specific regulations for the use of AI in conjunction with sensitive data contributes unequivocally to the perpetuation of these vulnerabilities in the Brazilian legal system, which lies in the urgency and exponential nature of the use of AI in vital sectors, such as health, education, and the labor market, where automated decisions directly impact fundamental rights, especially the right to equality and non-discrimination. The study will thus seek to contribute to a critical understanding of the gaps in legislation and suggest solutions that strengthen protection against algorithmic discrimination. Ultimately, it is considered that proposing technical and legal solutions could mitigate the risks of discrimination, promoting greater compatibility between the LGPD and contemporary technological practices.

Keywords: Digital Law, Data Protection, Anonymization, LGPD, Artificial Intelligence.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Agência Nacional de Proteção de Dados
ADMs	Armas de Destruição Matemáticas
IA	Inteligência Artificial
IA Gen	Inteligência Artificial Generativa
CC	Código Civil
CDC	Código de Direito do Consumidor
CEP	Código de Endereçamento Postal
CF	Constituição Federal
CPC	Código de Processo Civil
EBIA	Estrutura Brasileira de Inteligência Artificial
ECA	Estatuto da Criança e do Adolescente
EUA	Estados Unidos da América
GAN	Redes Adversariais Generativas
GDPR	General Data Protection Regulation
HD	*Habeas Data*
LGPD	Lei Geral de Proteção de Dados
LSCS	Lei Federal sobre Segurança Cibernética na Saúde
MCI	Marco Civil da Internet
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PbD	*Privacy by Design*
PEC	Proposta de Emenda à Constituição
PETs	Tecnologias de Aprimoramento da Privacidade
PL	Projeto de Lei
RIA	Regulamento de Inteligência Artificial da União Europeia
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
RGPD	Regulamento Geral de Proteção de Dados da União Europeia
TRF	Tecnologia de Reconhecimento Facial
UE	União Europeia

209

SUMÁRIO

1. INTRODUÇÃO

O advento da sociedade da informação e a consequente ascensão da *Inteligência Artificial* (IA) enquanto ferramenta ubíqua e transformadora impuseram um desafio epistemológico e prático ao edifício jurídico, exigindo uma reengenharia do universo normativo para tutelar os direitos fundamentais em face das novas dinâmicas tecnológicas[1].

Neste cenário, a *Lei Geral de Proteção de Dados Pessoais* (LGPD), Lei nº 13.709/2018, consolidou-se como um diploma de aplicação transversal, ancorado no imperativo de proteger a liberdade, a privacidade, e o *livre desenvolvimento da personalidade da pessoa natural*[2]. Contudo, a mera existência de um arcabouço legal não é, *per se*, uma panaceia diante da complexidade da IA e da fluidez do que se convencionou chamar de dado pessoal. É imperioso que o profissional do Direito assuma o papel de estrategista, comunicando-se com as demais áreas da sociedade, para lançar um olhar crítico sobre as insuficiências regulatórias e os riscos sistêmicos que ora se apresentam[3].

O ponto de partida desta análise reside na *ilusão da anonimização plena* e na complexidade do *dado pessoal sensível* na sistemática da LGPD, que bebe diretamente das fontes europeias (GDPR)[4]. A anonimização e o dado anonimizado são conceitos fundamentais, pois sua principal repercussão jurídica é o *afastamento de obrigações e encargos regulatórios* impostos pelo regime geral da Lei[5]. A anonimização, definida como a "*utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo*" (Art. 5º, XI, LGPD), não deve ser vista como um fim em si mesma, mas como *um processo contínuo baseado em riscos*[6].

É crucial sublinhar que o *ato inicial* do processo de anonimização já configura uma *operação de tratamento de dado pessoal*, o que atrai a incidência de princípios e regras da LGPD, notadamente a finalidade e a adequação[7]. A anonimização, portanto, não é capaz de

---

[1] PINHEIRO, Patricia Peck. *Direito digital* / Patricia Peck Pinheiro. – 7. ed. – São Paulo: Saraiva Educação, 2021. e-book. p. 32.
[2] LIMA, Ana Paula Canto de; SABOYA. Maria Beatriz. *Ensaios sobre direito digital, privacidade e proteção de dados* [livro eletrônico]. -- 1. ed. Império Jurídico, 2022. Recife, PE. p. 105.
[3] PINHEIRO, 2021, op. cit.
[4] LIMA; SABOYA, 2022, p. 229.
[5] BRASIL. Agência Nacional de Proteção de Dados. *Estudo técnico sobre anonimização de dados na LGPD: Análise Jurídica*. Brasília, DF: ANPD, 2023. 27 p. Versão 1.0. p. 6.
[6] BRASIL. Agência Nacional de Proteção de Dados. *Estudo técnico sobre anonimização de dados na LGPD: uma visão de processo baseado em risco e técnicas computacionais*. Brasília, DF: ANPD, 2023. 27 p. Versão 1.0. p. 4.
[7] BRASIL, ANPD, ref. 5, p. 6-7.

per se legitimar uma atividade de tratamento que fosse originalmente ilícita por carência de hipótese normativa, cabendo ao controlador informar, com clareza, a finalidade da futura anonimização[8].

A leitura atenta do art. 12 da LGPD revela a precariedade da segurança técnica. Um dado que foi anonimizado *não será considerado dado pessoal, salvo quando o processo de anonimização for revertido* utilizando exclusivamente meios próprios, ou *quando, com esforços razoáveis, puder ser revertido*[9]. Este critério do "esforço razoável" é um *conceito jurídico indeterminado normativo*, cujo conteúdo depende de preenchimento valorativo pelo aplicador do Direito[10]. O §1º do art. 12 estabelece um rol exemplificativo de aspectos objetivos a serem sopesados: *custo e tempo necessários para reverter o processo de anonimização*, considerando a tecnologia disponível. Tal dispositivo confirma que a LGPD adota a *teoria objetiva do conceito amplo de dado pessoal*, pois a avaliação da reidentificação deve levar em conta não apenas os meios próprios do agente de tratamento, mas também os meios e esforços razoáveis de *outras pessoas ou entidades*[11].

A doutrina e a *Agência Nacional de Proteção de Dados* (ANPD) concordam que, no atual estado da arte e desenvolvimento científico, existe um *consenso científico sobre a impraticabilidade de um cenário de ausência de risco de reidentificação*[12], especialmente considerando o volume de dados auxiliares (*auxiliary data*) disponibilizados publicamente via internet. A anonimização, portanto, não é um estado binário discreto de segurança plena, mas sim uma gestão contínua do risco[13].

O cenário de proteção se torna ainda mais crítico ao se analisar a categoria dos *dados pessoais sensíveis*. Estes dados — que incluem origem racial ou étnica, opiniões políticas, dados genéticos e *biométricos*, dados relativos à saúde ou à *vida sexual ou orientação sexual*, — exigem *proteção jurídica mais robusta*, uma vez que possuem um *elevado potencial lesivo*[14] e maior probabilidade de utilização discriminatória[15]. A própria criação dessa categoria especial decorreu de um impulso pragmático, ao constatar que a circulação de determinadas espécies de informação apresentaria um elevado potencial lesivo aos seus

[8] BRASIL, ANPD, ref. 5, p. 9.
[9] *Ibid.*, p. 20.
[10] *Ibid.*
[11] *Ibid.*, p. 21.
[12] *Ibid.*, p. 18.
[13] BRASIL, ANPD, ref. 6, p. 8.
[14] CARVALHO, Pedro Augusto Gil de; BOTELHO, Marcos César; TREJO, Jordy Arcadio Ramirez. *Gênero e sexualidade como dados sensíveis na Lei Geral de Proteção de Dados*. Revista Sapiência: Sociedade, Saberes e Práticas Educacionais, [S.l.], p. 274-297, 2023. p. 283.
[15] *Ibid.*, p. 284.

titulares, numa determinada configuração social. No setor financeiro, por exemplo, embora dados financeiros não sejam uma categoria especial na LGPD, *dados biométricos* são coletados para a prevenção à fraude, e são expressamente qualificados como sensíveis[16].

Uma crítica construtiva ao rol do Art. 5º, II, da LGPD reside na omissão da *identidade de gênero*. Embora o rol seja formalmente taxativo[17], a doutrina sustenta que a interpretação deve ser material, reconhecendo que a *identidade de gênero* e a *sexualidade* são dados sensíveis[18]. O tratamento inadequado de informações sobre o gênero de uma pessoa trans, por exemplo, pode ocasionar *grave violação à personalidade*, gerando contextos de discriminação para uma população já extremamente marginalizada[19].

Adota-se, destarte, a premissa de que o cerne do dado especial não é a sua natureza intrínseca, mas sim a *potencialidade discriminatória* que o tratamento oferece, à luz do pano de fundo sócio-histórico e jurídico[20]. Essa interpretação, embora possa levantar dúvidas sobre a segurança jurídica para os controladores, é necessária para elevar o padrão de proteção de um elemento tão caro à realidade social, rompendo com o manto da desigualdade formal[21].

Tamanha é a vulnerabilidade dos dados sensíveis que o *Relatório de Impacto à Proteção de Dados Pessoais* (RIPD) é indicado quando há tratamento de categorias especiais de dados em *larga escala*, ou quando o tratamento ocorre de *forma automatizada*, incluindo a definição de perfis[22]. O RIPD é um instrumento de *accountability* voltado a avaliar os riscos às liberdades civis e direitos fundamentais, exigindo que o controlador indique quais medidas e salvaguardas serão adotadas para a mitigação de riscos[23].

A IA, potencializada pelo *Big Data*, é o vetor principal que instrumentaliza e amplifica a potencialidade discriminatória dos dados sensíveis. A utilização incauta da IA pode ocasionar *resultados lesivos preocupantes*, *associados à discriminação algorítmica*[24]. O *Princípio da Não Discriminação*[25], previsto no art. 6º, IX da LGPD, é o elemento-chave para

---

[16] LIMA; SABOYA, 2022, p. 396.
[17] OLIVEIRA, Caio César de. *Apagamento, desindexação e esquecimento: a experiência brasileira na Internet. 2020*. 192 f. Dissertação (Mestrado em Direito Civil) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. p. 88.
[18] CARVALHO; BOTELHO; TREJO, 2023, p. 292.
[19] COSTA, Ramon; KREMER, Bianca. *Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial*. Direitos Fundamentais & Justiça, Belo Horizonte, ano 16, out. 2022, p. 158-159.
[20] CARVALHO; BOTELHO; TREJO, 2023, p. 283.
[21] COSTA; KREMER, 2022, p. 160.
[22] LIMA; SABOYA, 2022, p. 61-62.
[23] *Ibid,* p. 65-66.
[24] FRANÇA NETTO, Milton Pereira de; EHRHARDT JÚNIOR, Marcos. *Os riscos da discriminação algorítmica na utilização de aplicações de inteligência artificial no cenário brasileiro*. RJLB, Coimbra/Lisboa/São Paulo, ano 8, n. 3, 2022. p. 1271.
[25] LIMA; SABOYA, 2022, p. 123-124.

a tutela. Não obstante, o enfrentamento da discriminação algorítmica depara-se com a *complexidade tecnológica* e a *sinuosidade* que emana da *obscuridade típica dos algoritmos*[26].

A discriminação pode ser *direta* (como o uso evidente de dados sensíveis em análises preditivas) ou *indireta* (menos perceptível, como nos casos de generalização)[27]. Os enviesamentos nos resultados são gerados pela própria técnica de aprendizagem de máquina (*machine learning*), onde as máquinas estabelecem correlações com base em dados de treinamento que já contêm associações estereotipadas ou vieses sexistas. Tais vieses decorrem, em parte, de *decisões humanas em todas as etapas do processo*, desde o desenvolvimento do modelo até a interpretação do usuário[28].

A opacidade ou "efeito caixa-preta" (*black box*) do funcionamento dos modelos, especialmente nas técnicas de redes neurais profundas, constitui uma *barreira à adesão dos profissionais*, pois impede a *explicabilidade*[29]. Como bem questiona Alexandre Sayad, "*se somos incapazes de explicar decisões tomadas por sistemas autônomos, significa que não podemos justificá-las, o que é inconcebível em áreas cruciais da vida como crédito, emprego, saúde e justiça*"[30].

Por exemplo, no setor de saúde, como recomendar um diagnóstico automatizado sem saber como o sistema chegou ao resultado?[31]. No âmbito *da Tecnologia de Reconhecimento Facial* (TRF), a tecnologia pode intensificar contextos discriminatórios para populações vulneráveis, um problema que se agrava pela *ausência de transparência*[32] e pelos vieses de produção da própria tecnologia.

É neste ponto que a *compatibilidade entre a LGPD e a tecnologia* revela suas maiores tensões. O Direito deve buscar um sistema de proteção que transcenda a tutela meramente patrimonializada, avançando para um sistema de *cyberdireitos*[33]. A regulação precisa ser robusta o suficiente para lidar com a *opacidade, complexidade, autonomia e imprevisibilidade*

[26] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1274.
[27] *Ibid.*
[28] KAUFMAN, Dora. *Desmistificando a inteligência artificial*. Belo Horizonte: Autêntica, 2022. p. 37.
[29] *Ibid*. p. 281.
[30] SAYAD, Alexandre Le Voci. *Inteligência Artificial e Pensamento Crítico: Caminhos para a educação midiática*. 1. ed. São Paulo: Instituto Palavra Aberta. 2023. p. 81-82.
[31] KAUFMAN, 2022, p. 163.
[32] COSTA; KREMER, 2022, p. 159.
[33] CANTARINI, Paola; GUERRA FILHO, Willis Santiago; KNOERR, Viviane Coêlho de Séllos. *Direito e Inteligência Artificial: Fundamentos*. Vol. 4 – Por uma filosofia da inteligência artificial. Rio de Janeiro. Editora Lumen Juris. 2022. p. 391.

da IA. Conforme salientado em estudos sobre o tema, a IA não é uma fonte jurídica, e a tarefa essencial do raciocínio jurídico é determinar se certa regra se aplica a um caso particular[34].

O Direito da Concorrência, por exemplo, embora pareça distante, tem sido invocado como idôneo a garantir o tratamento da IA, mas reconhece-se o risco de se ignorar as repercussões e as relações de complementaridade que caracterizam a IA como realidade atual[35]. A grande dificuldade reside em criar *legislação que não envelheça e não se torne obsoleta* diante das modificações instantâneas, o que configura a "*obsolescência normativa*"[36].

No Brasil, o art. 20 da LGPD confere ao titular o direito de solicitar a *revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais* que afetem seus interesses[37]. Contudo, a efetividade desta garantia sofre um revés crítico, pois a Lei nº 13.853/2019 *vetou o dispositivo que previa a revisão por uma pessoa natural*, contrariando o GDPR (Art. 22) e os princípios da OCDE[38]. O veto foi justificado por razões utilitárias e econômicas, consideradas mais importantes do que a necessidade inafastável da *intervenção humana*, um pilar fundamental para mitigar riscos[39]. Esse veto enfraquece o exercício dos direitos humanos e de cidadania e ignora o fato de que algoritmos, baseados em cálculos probabilísticos, podem levar a *erros e desvios padrões*[40].

A opacidade dos algoritmos e a falta de revisão humana são características de sistemas *autoritários não regulados*[41], o que justifica a crítica de que a LGPD deixou margem para subjetividade onde deveria ter sido mais assertiva[42]. O controle *ex post* se limita a permitir ao usuário obter do controlador *informações cristalinas acerca dos critérios e procedimentos* implementados, mas até mesmo esse direito é excepcionado pela possível alegação de *sigilo comercial e industrial*[43], o que leva à inevitável *colisão com outros direitos fundamentais*[44].

---

[34] GUIMARÃES, Maria Raquel; PEDRO, Rute Teixeira. *Direito e Inteligência Artificial*. Editora Almedina. Coimbra. out. 2023. p. 306.
[35] *Ibid*. p. 604.
[36] MARQUES, Claudia Lima; MARTINS, Guilherme Magalhães; MARTINS, Fernando Rodrigues (Coord.). *10 anos marco civil da internet: avaliando impactos e desafios* [recurso eletrônico]. Indaiatuba, SP: Editora Foco, 2024. 296 p. ISBN: 978-65-6120-192-6 (Ebook). p. 122-123.
[37] LIMA; SABOYA, 2022, p. 482.
[38] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 336.
[39] *Ibid*. p. 223.
[40] CANTARINI; GUERRA FILHO; KNOERR. 2022, ref. 38.
[41] COSTA; KREMER, 2022, p. 157.
[42] PINHEIRO, 2021, p. 285.
[43] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1306-1307.
[44] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 339.

Neste contexto de incertezas e lacunas, torna-se imperativo delinear *Diretrizes para a Mitigação de Riscos* que transcendam a mera observância da lei fria, adotando uma postura ética e proativa.

Em prévio arremate, esta inicial incursão sobre a IA, anonimização e LGPD demonstra que, embora o Brasil disponha de um arcabouço normativo robusto (LGPD) e de uma agência reguladora (ANPD) empenhada em fiscalizar riscos[45], a *guarda dos direitos fundamentais* na era digital não é uma batalha vencida. O direito de oposição ao tratamento, o direito de anonimização e o direito de eliminação de dados (Art. 18, LGPD)[46], embora sejam ferramentas importantes para o controle do fluxo de tratamento, não são sinônimos de um absoluto "*direito ao esquecimento*". Pelo contrário, o foco deve se concentrar no aperfeiçoamento de tais ferramentas e na ponderação criteriosa dos princípios[47].

A IA, em sua complexidade, impõe o sempre difícil exercício de adaptar uma realidade nova aos velhos edifícios erigidos em tempos idos, testando os limites e fronteiras do Direito Civil e da Responsabilidade[48]. A opacidade algorítmica e a flexibilização da revisão humana por questões utilitárias são indicativos de que a *segurança jurídica* e a *proteção dos mais vulneráveis* (como as crianças, os idosos, ou minorias sujeitas à vigilância opressiva)[49] ainda carecem de uma tutela efetiva e incondicional, exigindo uma *análise holística*, e a contínua busca por um cabal equilíbrio entre todos os interesses em jogo[50].

[45] BRASIL. ANPD. *Nota técnica n. 19/2023/FIS/CGF/ANPD*. [S.l.]: ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-19-2023-fis-cgf-anpd.pdf.
[46] PINHEIRO, 2021, p. 97.
[47] OLIVEIRA, 2020. p. 153.
[48] GUIMARÃES; PEDRO, 2023. p. 445.
[49] MARQUES; MARTINS; MARTINS, 2024, p. 332.
[50] GUIMARÃES; PEDRO, *Ibid.*

2. ANONIMIZAÇÃO E DADOS SENSÍVEIS NA LGPD

2.1. Definições legais e técnicas

O direito, enquanto fenômeno social que reflete as transformações culturais e comportamentais da sociedade, depara-se, na quadra contemporânea, com o inexorável e vertiginoso avanço das tecnologias digitais, notadamente a IA e o manuseio maciço de dados, que ensejam a reengenharia do universo jurídico[51].

Nesse panorama, a discussão sobre a *Anonimização* e *Dados Sensíveis* sob a égide da LGPD, revela-se *mister* não apenas de subsunção normativa, mas de profunda reflexão ético-constitucional, dada a latente ameaça aos direitos fundamentais de liberdade, intimidade e o livre desenvolvimento da personalidade[52].

Inicialmente, a OCDE iniciou as discussões sobre a temática e publicou as *diretrizes sobre a proteção da privacidade* como expressão de uma mentalidade de preocupação com o poder da computação em manipular dados[53]. Essas diretrizes, conhecidas como *Guidelines on the Protection of Privacy and Transborder of Personal Data*[54], demonstram que o debate sobre privacidade e proteção de dados em nível global são fundamentais à manutenção dos direitos dos homens, promovendo no ano seguinte o reconhecimento da Convenção 108, o primeiro texto legal internacional para adesão dos países europeus e não europeus[55].

Ainda, cumpre revisitar os alicerces jurídicos que sedimentaram o entendimento de que a informação pessoal deve ser resguardada com rigor. O arcabouço normativo brasileiro, desde a *Constituição Federal de 1988*, já assegurava, em seu Art. 5º, X, a *inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas*[56]. A doutrina constitucionalista, ademais, indica que a tutela da inviolabilidade dos dados informáticos e telemáticos encontra previsão no Art. 5º, XII. A primeira materialização processual desse direito no âmbito da

---

[51] PINHEIRO, 2021, p. 31.

[52] CASALI SILVA, Felipe. *Proteção de Dados Pessoais na Era da Inteligência Artificial*. 2023. 74 f. Monografia (MBA em Inteligência Artificial e Big Data) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2023. p. 25.

[53] BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. In: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo (Coords. gerais). Enciclopédia jurídica da PUC-SP. São Paulo: Pontifícia Universidade Católica de São Paulo, 2022. Tomo: Direito Internacional. Coords. de tomo: Cláudio Finkelstein; Clarisse Laupman Ferraz Lima. 1. ed. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais.

[54] LIMA; SABOYA, 2022, p. 275.

[55] Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Disponível em <http://www.oecd.org/sti/ieconomy/15590254.pdf>.

[56] BRASIL. Constituição da República Federativa do Brasil: de 5 de outubro de 1988. Brasília, DF: Presidência da República, 1988.

informação deu-se com o *Habeas Data* (Art. 5º, LXXII), instrumento que confere ao titular o direito de conhecer e retificar dados próprios constantes em registros ou bancos de dados de entidades governamentais ou de caráter público[57].

Paralelamente ao desenvolvimento constitucional pátrio, o cenário internacional já delineava a necessidade de proteção especializada. A *Diretiva 95/46/CE* do Parlamento Europeu e do Conselho, de 1995, estabeleceu a premissa de que a aplicabilidade dos princípios de proteção não recairia sobre *informações anônimas* ou dados tornados anônimos, de tal modo que o titular não pudesse ser identificado[58]. Para aferir a identificabilidade, já se consideravam os *meios suscetíveis de ser razoavelmente utilizados*, critério que posteriormente seria incorporado na LGPD. O direito europeu, *ab initio*, buscou uniformizar o tratamento de dados pessoais, elevando-o à condição de direito fundamental[59].

Em um passo significativo para a tutela digital no Brasil, sobreveio o *Marco Civil da Internet* (Lei nº 12.965/2014). Embora o MCI tenha estabelecido princípios fundamentais como a *proteção da privacidade e dos dados pessoais*[60], o diploma legal demonstrou insuficiência no trato da *responsabilidade civil por moderação por IA*[61], preocupando-se mais em delimitar a responsabilidade do provedor somente após a notificação pelo ofendido (o modelo *notice and take down judicial* do Art. 19) do que em prever diretrizes para o balizamento de conteúdo automatizado. Em um mundo onde a *plataformização da vida em sociedade* transformou entes privados transnacionais em verdadeiros "*julgadores*"[62], a ausência de um arcabouço normativo que prevenisse o dano a priori já sinalizava uma deficiência do paradigma protetivo da informação[63].

Consequentemente, a LGPD surge como a resposta legislativa à lacuna deixada pelo MCI e como reflexo direto do GDPR, caracterizando um evidente *Brussel Effect* em território nacional[64]. A LGPD consolida o *conceito amplo de dado pessoal* em seu Art. 5º, I, definindo-o como a "*informação relacionada a pessoa natural identificada ou identificável*"[65]. Essa abordagem expansionista, que trata os dados identificados e identificáveis como equivalentes,

---

[57] OLIVEIRA, 2020. p. 57.
[58] MACHADO, Diego; DONEDA, Danilo. *Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no Direito Brasileiro*. Revista de Direito Civil Contemporâneo. vol. 23/2020, p. 95 – 140, abr – jun 2020. DTR\2021\207. p. 4.
[59] MACHADO; DONEDA, 2020. *Ibid.*
[60] PINHEIRO, 2021, p. 61.
[61] MARQUES; MARTINS; MARTINS, 2024, p. 255.
[62] *Ibid.*, p. 298.
[63] *Ibid.*, p. 159.
[64] *Ibid.*, p. 155.
[65] MACHADO; DONEDA, 2020, p. 2.

demonstra a opção do legislador por uma tutela que transcende a mera vinculação imediata, englobando a potencialidade de identificação futura[66].

Nessa conformação, o legislador pátrio estabeleceu a categoria dos *Dados Pessoais Sensíveis* (Art. 5º, II), cuja delimitação é crucial, pois seu tratamento indevido acarreta um *risco de discriminação abusiva*[67]. São dados que, por sua natureza (origem racial ou étnica, convicção religiosa, dados de saúde, vida sexual, genéticos ou biométricos), possuem grande potencial de *violação de direitos fundamentais* A LGPD, ao se fundamentar no *Princípio da Não Discriminação* (Art. 6º, IX), exige um rigor maior no tratamento dessas informações. Contudo, percebe-se uma *lacuna e deficiência de esteio* no Art. 5º, II, que não inclui expressamente a *identidade de gênero*[68]. A doutrina, todavia, argumenta que, por meio de uma *análise pragmática e material sobre os efeitos* em termos de produção de desigualdade, elementos como identidade de gênero e orientação sexual devem ser interpretados como dados sensíveis, dada a *potencialidade discriminatória* que o tratamento indevido pode gerar e o histórico de agressões sociais. Esse desideratum hermenêutico é necessário para garantir a *igualdade material*[69].

Em contrapartida à tutela dos dados pessoais, a LGPD introduz a figura da *Anonimização*, definida no Art. 5º, XI, como a "*utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo*"[70]. O *dado anonimizado* — ou seja, o resultado desse processo técnico — não é considerado dado pessoal para os fins da LGPD, resultando no *afastamento dos encargos regulatórios*[71].

Entretanto, a LGPD, em uma visão que demonstra expertise técnica e insight jurídico, consagra a crítica à ilusão da anonimização ao prever o *teste de reversibilidade* no Art. 12, caput: o regime protetivo será aplicado se o processo for *revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido*[72]. Essa ressalva legal aponta para a inevitabilidade de um *modelo ou abordagem baseada em riscos de*

---

[66] BRASIL, ANPD, ref. 5, p. 12.
[67] CARVALHO; BOTELHO; TREJO, 2023, p. 283.
[68] KELLER, Elaine Cristine Zordan. *A tutela da identidade de gênero na LGPD: uma análise na perspectiva de dado sensível*. 2022. 90 f. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) – Programa de Pós-Graduação Profissional Stricto Sensu em Direito, Justiça e Desenvolvimento, Instituto Brasiliense de Direito Público (IDP), São Paulo, 2022. p. 46.
[69] CARVALHO; BOTELHO; TREJO, 2023, *Ibid.*
[70] BRASIL, ANPD, ref. 5, p. 6.
[71] *Ibid.*, p. 4.
[72] *Ibid.*, p. 6.

(re)identificação[73], reconhecendo o consenso científico sobre a impraticabilidade de um cenário de ausência de risco zero[74].

O conceito de "*esforços razoáveis*" (Art. 12, § 1º) é, por sua natureza, *jurídico indeterminado*, e deve ser aferido com base em fatores objetivos, tais como *custo e tempo* necessários para reverter o processo, em consonância com as *tecnologias disponíveis*[75]. A *ilicitude* é um fator limitador desse esforço, pois a prática de crimes cibernéticos ou atos ilícitos configura *meios e esforços irrazoáveis* para a reversão. A LGPD, ao requerer que se considere não apenas os meios próprios do controlador, mas também os *meios e esforços razoáveis de outrem*, aponta para a *teoria objetiva do conceito amplo de dado pessoal*[76].

Ademais, *mister* se faz distinguir a anonimização da *pseudonimização*. Esta última, prevista no Art. 5º, XIII, é o tratamento que impede a associação direta ao titular, "*senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro*" [77]. Por conseguinte, um dado pessoal *criptografado ou encriptado*, embora ininteligível a terceiros, *não configura dado anonimizado*, mas sim, *dado pseudonimizado*, pois o agente que detém a chave criptográfica possui os *meios próprios* para revertê-lo, aplicando-se, *prima facie*, o estatuto de proteção de dados pessoais, ainda que de forma modulada[78].

A discussão sobre o tratamento lícito também circunda os princípios basilares. A LGPD exige que o ato inicial do processo de anonimização configure uma *operação de tratamento de dado pessoal*, fazendo incidir princípios como *Finalidade* (Art. 6º, I) e *Adequação* (Art. 6º, II). A finalidade de anonimização deve ser informada de forma legítima, específica, explícita e informada ao titular[79]. Outrossim, o *Princípio da Necessidade* (Art. 6º, III) impõe que o tratamento seja limitado ao mínimo necessário, o que exige uma avaliação prévia para *verificar se o propósito pode ser alcançado com o uso mínimo de dado pessoal*[80]. Esse *mínimum* de coleta e uso é, a *contrario sensu*, uma medida preferível ao apagamento total, funcionando como uma ferramenta de aperfeiçoamento dos direitos do titular[81].

[73] BRASIL, ANPD, ref. 5, p. 21-22.
[74] BRASIL, ANPD, ref. 6, p. 16.
[75] BRASIL, ANPD, ref. 5, p. 20.
[76] *Ibid.*, p. 21-22.
[77] MACHADO; DONEDA, 2020, p. 6.
[78] Ibid.
[79] BRASIL, ANPD, ref. 5, p. 22.
[80] Ibid.
[81] OLIVEIRA, 2020. p. 137.

A crítica construtiva ao tema exige que se compreenda o contexto fático-econômico no qual a LGPD se insere: a lógica do Capitalismo de Vigilância[82]. Este sistema reivindica *unilateralmente a experiência humana como matéria-prima gratuita* para tradução em dados comportamentais, que são manufaturados em produtos de predição[83]. Nesse cenário, a privacidade é degradada, e o indivíduo é objetificado e moldado em seus comportamentos. Essa dinâmica de extração massiva de dados leva ao *risco de feedback loop de injustiça*, onde vieses históricos e sociais incutidos nos *datasets* de treinamento da IA resultam em decisões automatizadas que perpetuam a *discriminação*[84].

O uso da IA, especialmente em áreas sensíveis, como saúde e segurança pública, ilustra a urgência dessa preocupação. A *Tecnologia de Reconhecimento Facial* (TRF), por exemplo, que trata *dados biométricos* (Art. 5º, II), demonstra-se um foco de risco crítico de potencial altamente *discriminatório e lesivo*[85]. Os algoritmos podem reforçar o racismo e a violência ao operar com base em estereótipos, haja vista que o reconhecimento facial tem apresentado vieses preocupantes. A carência de *transparência e explicabilidade* (Art. 6º, VI) nos algoritmos e nas bases de dados utilizadas agrava o problema[86].

Nesse diapasão, a tutela do titular contra a tomada de *decisões automatizadas* que o afetem significativamente é uma garantia central, preconizada tanto pelo GDPR (Art. 22) quanto implicitamente pela LGPD (Art. 20). O titular deve ter o direito de obter *informações claras e adequadas* sobre os critérios e procedimentos para a decisão automatizada[87]. A ausência de clareza nesse tratamento e a opacidade algorítmica configuram um desafio sine qua non para o exercício dos direitos[88].

O enfrentamento desse *dilemma Utilidade x Anonimização*[89], que busca o compromisso entre o grau de utilidade do dado e o grau de anonimização, torna-se a missão precípua do regulador. Com a instituição da ANPD, essa entidade se tornou peça-chave para zelar, orientar e fiscalizar o cumprimento da LGPD. Em alinhamento com a complexidade do tema, a ANPD definiu para o biênio *2024-2025* a prioridade de temas como *Anonimização e Pseudonimização* (Tema 11) e *Inteligência Artificial e Tratamento de Dados Pessoais* (Tema 3)[90]. Essa priorização

[82] ZUBOFF, Shoshana. *A era do capitalismo de vigilância*. Tradução de Rafael Abraham. 1. ed. Rio de Janeiro: Editora Intrínseca, 2021. p. 271.
[83] *Ibid.*
[84] COSTA; KREMER, 2022, p. 152.
[85] PINHEIRO, 2021, p. 160.
[86] COSTA; KREMER, 2022, op. cit.
[87] KELLER, 2022, p. 73-74.
[88] BRASIL. ANPD, ref. 45, p. 8.
[89] BRASIL, ANPD, ref. 6, p. 5.
[90] BRASIL. ANPD, ref. 45, p. 8.

se justifica pela *atualidade e gravidade* dos riscos envolvidos, demandando ações que vão desde a fiscalização até a elaboração de guias e normas[91].

Em suma, a LGPD estabeleceu um regime protetivo que, embora robusto em sua inspiração principiológica e na definição de dados sensíveis e técnicas de mitigação, demanda constante *aperfeiçoamento* e *esforço interpretativo*, ao prever a responsabilidade civil objetiva para o agente de tratamento, reforça o princípio da responsabilização e prestação de contas (*accountability*)[92].

Contudo, a efetividade da proteção de dados sensíveis e o controle da IA dependerão da capacidade de se abandonar a retórica simplista, como a utilização indiscriminada do conceito de "*direito ao esquecimento*" para justificar o apagamento de dados ou a desindexação[93], e de se focar no *aperfeiçoamento das ferramentas trazidas pela LGPD*, tais como a correção, a anonimização e o princípio da mínima coleta de dados pessoais[94]. A anonimização, *in fine*, não é uma solução de risco zero, mas um processo contínuo baseado em risco, exigindo *privacy by design* e constante avaliação técnica[95].

O desafio reside, portanto, na garantia de que a *justiça seja imparcial* e de que a aplicação do direito digital consiga *harmonizar a liberdade responsável com a punição do abuso*[96], sem que a tecnologia se torne um fim em si mesmo, mas um instrumento a serviço da dignidade da pessoa humana. Tal empreendimento exige a aplicação do Direito à luz dos princípios da adequação, necessidade e proporcionalidade em sentido estrito, ponderando o interesse público, a liberdade de informação e os direitos da personalidade em cada caso concreto[97]. O Judiciário e a ANPD, nesse *múnus* árduo, são chamados a definir os limites entre o que é lícito, necessário e proporcional, de modo a evitar que a vagueza e imprecisão conceitual ofusquem a efetiva tutela dos direitos constitucionais[98].

2.2. Limites práticos da anonimização

A LGPD estabeleceu a *anonimização* como uma medida de salvaguarda essencial, definindo-a como o processo pelo qual o dado perde a possibilidade de associação, direta ou

[91] BRASIL. ANPD, ref. 45, p. 8.
[92] PINHEIRO, 2021, p. 286.
[93] OLIVEIRA, 2020. p. 85.
[94] *Ibid.*, p. 134.
[95] BRASIL, ANPD, ref. 6, p. 16.
[96] PINHEIRO, 2021, p. 305.
[97] OLIVEIRA, 2020. p. 144-145.
[98] *Ibid.*, p. 108.

indireta, a um indivíduo. Consoante a disciplina jurídica pátria, os princípios de proteção de dados não se aplicam às informações anônimas, que não digam respeito a uma pessoa identificada ou identificável[99]. No entanto, a investigação crítica sobre o tema demonstra, com o devido respeito, que a aplicação prática da anonimização, especialmente em um cenário dominado pela IA e pelo *Big Data*, revela-se, em muitos casos, uma *ilusão de proteção*.

O principal limite prático da anonimização reside no seu caráter *dinâmico e contextual*. O que é considerado anonimizado hoje pode ser reidentificado amanhã, devido ao avanço contínuo das tecnologias de processamento de dados[100].

Para determinar se uma pessoa singular é identificável, impõe-se a consideração de *todos os meios suscetíveis de serem razoavelmente utilizados*, incluindo a seleção tanto pelo responsável pelo tratamento quanto por terceiros. Essa avaliação deve considerar fatores objetivos, como os custos, o tempo necessário e, crucialmente, a tecnologia disponível à data do tratamento dos dados e sua evolução subsequente[101].

O Grupo de Trabalho do Artigo 29 (WP 29) já destacava que a anonimização é inerente à existência de um fator de risco. A ciência da computação tem demonstrado que os dados anonimizados mantêm o risco latente de se transmutarem novamente em dados pessoais. Esta vulnerabilidade advém do chamado *efeito mosaico*, no qual a agregação de diversos fragmentos de informação, isoladamente anônimos, permite a reconstrução (reidentificação) da imagem (sujeito) do quebra-cabeça[102].

Destarte, o processo de anonimização deve ser abordado, por padrão, como um *processo contínuo baseado em riscos*, e não meramente como a aplicação isolada de técnicas. A LGPD e o GDPR, ao exigir um modelo de avaliação de risco para o tratamento, reconhecem implicitamente que a anonimização absoluta é um ideal técnico de difícil, senão impossível, concretização[103].

Cumpre ressaltar que a insuficiência se agrava no contexto da IA, devido às *limitações das técnicas clássicas de anonimização*[104]. Muitas das técnicas tradicionais, como supressão (retirada de identificadores diretos) ou generalização (agrupamento de dados em categorias

[99] OLIVEIRA, 2020. p. 4-5.
[100] MACHADO; DONEDA, 2020, p. 6.
[101] MACHADO, Diego; DONEDA, Danilo. *Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados*. , vol. 1, p. 99-128, dez. 2018. p. 3.
[102] BRASIL, ANPD, ref. 6, p. 20.
[103] *Ibid*. p. 16.
[104] *Ibid.* p. 12.

mais amplas)[105], foram concebidas e limitam-se a lidar com *dados textuais estruturados e estáticos*[106].

De acordo com a declaração emitida pelo *Gabinete para Protecção de Dados Pessoais* (GPDP) do Governo de RAEM, em Macau, a IA, por outro lado, trabalha massivamente com dados em diversos formatos, incluindo imagens, áudio, dados biométricos e dados em fluxo[107]. E, nesse caso, a aplicação de técnicas tradicionais a formatos complexos (como máscaras de olhos ou pixelação em imagens) indicados como recomendados no Estudo Técnico da ANPD, introduz desafios adicionais, demandando técnicas de anonimização completamente diferentes.

Ademais, a própria utilidade dos dados é frequentemente perdida quando a anonimização é aplicada em níveis de rigor suficientes para mitigar o risco de reidentificação[108]. A generalização excessiva, por exemplo, embora reduza o risco de reidentificação, leva à *perda da precisão dos dados*[109], tornando-os pouco úteis para os modelos de *machine learning* que dependem da riqueza e granularidade das informações[110].

Consequentemente, os exemplos de falha na prática da IA são inimagináveis. No cenário de IA, observa-se que o aprendizado de máquina supervisionado busca padrões e correlações em conjuntos de dados (dados de interesse) para predizer um resultado (variável-alvo). Se o conjunto de dados utilizado para o treinamento for escasso ou sub-representativo de determinados grupos, o modelo pode falhar tecnicamente, resultando em discriminação não intencional. Um exemplo de falha técnica, que gerou enviesamento, é o caso em que um algoritmo falhou em reconhecer usuários asiáticos, o que se deu, possivelmente, pela *escassez de imagens de pessoas asiáticas* no conjunto de dados de treinamento[111].

Logo, ao processar dados de forma probabilística e até mesmo "anonimizada," pode gerar o surgimento de algoritmos de *policiamento preditivo*, os quais representam um terreno fértil para práticas discriminatórias, intensificando a marginalização de grupos historicamente oprimidos[112].

Destarte, não se trata apenas de uma falha legal, mas de uma *vulnerabilidade tecnológica*. Mesmo quando o dado é pseudonimizado — uma técnica que permite uma análise

---

[105] BRASIL, ANPD, ref. 6, p. 20.
[106] *Ibid*. p. 16.
[107] MACAU. Gabinete Para a Protecção de Dados Pessoais. *Guia para técnicas básicas de anonimização de dados*. [Tradução de: *GUIDE TO BASIC DATA ANONYMISATION TECHNIQUES*, publicado pela Personal Data Protection Commission of Singapore, 2018]. Macau: GPDP, 2019. 42 p., p. 4-5.
[108] *Ibid*. p. 11-12.
[109] BRASIL, ANPD, ref. 6, p. 22.
[110] CASALI SILVA, 2023. p. 25.
[111] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1297-1300.
[112] *Ibid*. p 1300-1303.

geral, mantendo as informações adicionais separadas para possibilitar a atribuição a um titular específico —, o risco persiste, e o dado ainda é reputado como informação pessoal. O dado pseudonimizado é uma etapa de segurança que deve ser considerada, mas não substitui a anonimização ou elimina o risco[113].

Concisamente, a promessa de irreversibilidade da anonimização, tal como esperada pela LGPD, é desafiada pela própria arquitetura da internet e pela voracidade dos sistemas de IA, o que exige dos agentes de tratamento a adoção de medidas técnicas e organizativas adequadas, como o *privacy by design* e a minimização de dados[114]. A ANPD deve dispor sobre padrões e técnicas para o processo de anonimização, reconhecendo que uma abordagem baseada em risco é imprescindível para mitigar a *discriminação algorítmica*[115].

2.3. A relação entre dados sensíveis e discriminação

Com o advento da LGPD, estabeleceu um marco regulatório essencial no ordenamento jurídico brasileiro, visando, precipuamente, a proteção dos direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade[116]. O diploma legal busca, outrossim, o equilíbrio entre as liberdades essenciais à inovação e o indispensável amparo aos dados pessoais[117].

Neste contexto de proteção, o legislador conferiu uma disciplina jurídica mais rigorosa ao tratamento dos *dados pessoais sensíveis*. A rigor, a criação desta categoria dos dados sensíveis não foi isenta de críticas doutrinárias, porquanto se afirma que, *in ultima ratio*, é impossível definir *ex ante* os efeitos do tratamento de uma informação, e que o dado, *per se*, não é discriminatório — mas o uso que dele se faz o pode ser[118]. Não obstante, a elaboração da categoria dos dados sensíveis atende à necessidade premente de delimitar uma área na qual a

[113] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas, L 119, p. 1-88, 4 de maio de 2016.
[114] OYADOMARI, Winston; COSTA, Ramon Silva; RIBEIRO, Manuella Maia. Proteção de dados pessoais: privacidade e confiança no ambiente digital. Panorama Setorial da Internet, [S.l.]: Cetic.br|NIC.br, ano 15, n. 2, jun. 2023. p. 23.
[115] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1303.
[116] CASALI SILVA, 2023, p. 26.
[117] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1305.
[118] MARINHO, Letícia Ramos. Ausência de regulamentação da IA para a proteção de dados pessoais sensíveis de saúde: análise sobre danos aos titulares. Revista Sapiência: Sociedade, Saberes e Práticas Educacionais, [S.l.], p. 274-297, 2023. p. 6.

probabilidade de utilização discriminatória da informação demonstra-se significativamente maior[119].

Com efeito, a principal razão de ser da distinção entre dados pessoais comuns e dados sensíveis reside, justamente, na necessidade de garantir que o tratamento se dê em conformidade com o princípio basilar da *não discriminação*, previsto no art. 6º, IX, da LGPD, que proíbe o tratamento para fins ilícitos ou abusivos[120]. A tutela rigorosa desses dados revela que o princípio da igualdade material é um valor central para a proteção de dados, visando coibir processos sociais de exclusão e segregação que dados de natureza especial são aptos a facilitar[121].

Quando sistemas automatizados, conhecidos como *Armas de Destruição Matemáticas,* (*ADMs*), ingerem essas informações, mesmo que supostamente anonimizadas ou pseudonimizadas, a ameaça de reidentificação e a manifestação de vieses preconceituosos tornam-se agudas[122].

O risco mais insidioso provém da *discriminação algorítmica indireta*, aquela que não se configura com intenção maliciosa, mas que é o resultado inevitável de sistemas que aprendem e reforçam iniquidades sociais históricas presentes nos *datasets* de treinamento. A utilização de algoritmos no cotidiano, como na seleção e admissão de empregados e estudantes, torna-se um palco de preocupantes resultados lesivos, muitas vezes quase imperceptíveis ao cidadão comum[123].

No domínio da saúde, por exemplo, a Lei dos Portadores de Deficiências (ADA, nos EUA) já proíbe exames médicos no processo seletivo, contudo, há o desafio premente de *atualizar a legislação para abarcar testes de personalidade de Big Data* e pontuações de saúde previstas por IA, que escapam das proibições legais vigentes[124]. Isso demonstra que os sistemas de IA, ao quantificar aspectos ricos do comportamento, transformam a informação "suave" em dados preditivos compreensíveis para instituições formais, podendo gerar modelos que antecipam, por exemplo, a probabilidade de um empréstimo ser pago ou não[125].

Ademais, o uso de *proxies* (variáveis substitutas) é um dos métodos pelos quais os vieses se perpetuam. Um sistema de classificação de crédito baseado em redes sociais, embora aparentemente neutro em sua matemática, pode trabalhar contra um indivíduo de classe

---

[119] MARINHO, 2023, p. 8.
[120] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, *loc. cit.*
[121] CARVALHO; BOTELHO; TREJO, 2023, p. 285.
[122] O'NEIL, Cathy. *Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. 1. ed. Santo André, SP: Editora Rua do Sabão, 2020. p. 15-16.
[123] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1288-1292.
[124] O'NEIL, 2020, p. 197.
[125] ZUBOFF, 2021. p. 214-215.

socioeconômica mais baixa que tem amigos desempregados ou com histórico criminal, em contraste com um recém-formado com amigos investidores, perpetuando, assim, a estratificação social e suas injustiças. O algoritmo, neste contexto, atua como um espelho que reflete e, pior, amplifica os preconceitos inerentes aos dados com os quais foi alimentado[126].

A urgência do debate se torna ainda mais evidente ao se considerar que a própria LGPD não esgotou as categorias de dados sensíveis. O rol do art. 5º, II, ainda que concebido como taxativo por parte da doutrina, não incluiu explicitamente a *identidade de gênero e a sexualidade*, apesar de seu elevado potencial para estigmatização, exclusão e segregação, o que exige um controle rigoroso[127]. Negar a estas informações a qualidade de dado sensível dificulta a implementação de políticas públicas e a coibição da violência e discriminação contra a população LGBTQIA+[128]. O tratamento massivo desses dados, como os biométricos e raciais, especialmente em tecnologias de vigilância, como o *reconhecimento facial* (*TRF*), gera falhas técnicas significativas com vieses raciais, sendo menos acurados para pessoas com tons de pele mais escuros[129]. Tais tecnologias, por seu alto potencial opressivo, intensificam problemas já radicados na sociedade brasileira marcada por discriminações de raça, classe, gênero e orientação sexual[130].

Diante da natureza dinâmica e contextual da anonimização, que é constantemente desafiada pela reidentificação, a ANPD reconheceu a necessidade de uma *abordagem baseada em riscos de (re)identificação* para qualquer processo de anonimização. A anonimização não é uma solução estática e final, mas sim um processo que exige a observância dos princípios da LGPD, como a finalidade e a adequação. Apenas análises baseadas em evidências e em cenários objetivos da realidade, que considerem os meios e esforços razoáveis de reidentificação por qualquer pessoa ou ente (não apenas o controlador), podem garantir a proteção necessária[131].

Portanto, a LGPD, ao postular a não discriminação, exige que o ordenamento jurídico não se limite à igualdade formal, mas seja um vetor da *igualdade material*, antecipando os potenciais riscos de violação[132]. É imperativo que a regulamentação futura da IA e a fiscalização da LGPD se concentrem em exigir a *transparência* e a *explicabilidade* dos sistemas[133], garantindo que os dados sensíveis não se tornem ferramentas para manter ou intensificar o *status*

[126] O'NEIL, 2020, p. 68-115.
[127] CARVALHO; BOTELHO; TREJO, 2023, p. 289-290.
[128] KELLER, 2022. p. 46.
[129] COSTA; KREMER, 2022, p. 154-155.
[130] *Ibid.* p. 157.
[131] BRASIL. ANPD, 2023, ref. 5, p. 21.
[132] CARVALHO; BOTELHO; TREJO, 2023, p. 283.
[133] COSTA; KREMER, 2022, p. 152.

quo discriminatório[134]. O combate a esses enviesamentos nocivos e não intencionais requer medidas complementares, como a expansão de estudos sobre a temática e a exigência de *intervenção humana* nos processos de revisão de decisões automatizadas que afetem significativamente os direitos dos titulares[135].

[134] O'NEIL, 2020, p. 115.
[135] COSTA; KREMER, 2022, p. 161.

3. INTELIGÊNCIA ARTIFICIAL E DISCRIMINAÇÃO ALGORÍTIMICA

3.1. Funcionamento dos sistemas baseados em IA

O debate sobre a Inteligência Artificial (IA) e o seu potencial intrínseco de gerar discriminação algorítmica não é um mero exercício de futurologia jurídica, mas sim uma análise premente das consequências da evolução técnica sobre a ordem social e o arcabouço normativo de proteção de direitos fundamentais[136]. O campo da IA, que hoje permeia nossa comunicação, sociabilidade e até sistemas automatizados de decisão, configura uma nova mediação entre o ser humano e o mundo, exigindo uma crítica apurada acerca de como essa tecnologia, em sua essência, molda a realidade[137].

Historicamente, a gênese desse campo remonta à metade do século XX, com o propósito explícito de mimetizar o intelecto humano. Embora a literatura cite os estudos e experimentos do cientista britânico Alan Turing, com sua provocação sobre a capacidade das máquinas pensarem em "*Computing Machinery and Intelligence*", como parte da pré-história da IA[138], o termo específico só foi cunhado por John McCarthy, em 1955, para diferenciar a nova área de conceitos correlatos, como *automata* (transformação de objetos materiais em máquinas moventes) ou *cibernética* (associada a feedback e controle)[139]. O marco fundacional, o *Dartmouth Summer Research Project on Artificial Intelligence* (1956), estabeleceu o pressuposto de que todos os aspectos do aprendizado ou da inteligência humana poderiam, em princípio, ser descritos tão precisamente que permitiriam a simulação por uma máquina[140]. McCarthy, mais tarde, definiu a IA como *a ciência e a engenharia de fazer máquinas inteligentes*, especialmente programas de computador inteligentes[141].

O que assistimos hoje, contudo, transcende a programação linear imaginada nos primórdios da IA pós-Segunda Guerra Mundial, quando a tecnologia se tornou um projeto efetivo impulsionado pelo desenvolvimento de computadores modernos[142]. A evolução técnica foi marcada por uma *ruptura epistemológica*, migrando da inferência mecânica linear para uma *operação digital recursiva*[143]. A IA contemporânea, em especial a modalidade de *machine*

---

[136] *REVISTA JURÍDICA DA PRESIDÊNCIA*. Brasília, DF: Centro de Estudos Jurídicos da Presidência, v. 27, n. 141, jan./abr. 2025. Dossiê. p. 46.
[137] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 143.
[138] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p.76.
[139] *Ibid.*, p. 139.
[140] *Ibid.*
[141] SAYAD, 2023, p. 60.
[142] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 305.
[143] SAYAD, 2023, p. 25.

learning (aprendizado de máquinas), é regida por um *sistema probabilístico*, e não determinístico[144]. Essa habilidade dos algoritmos de *aprender com dados* é o que permite a automação de atividades sem a necessidade de uma programação exaustiva por humanos[145]. Tais sistemas, treinados em *imensos conjuntos de dados* (o *big data*), funcionam por meio de modelos estatísticos que extraem propriedades e estabelecem correlações para realizar *predições* sobre comportamentos, interesses ou tendências futuras[146].

O funcionamento mais complexo e, paradoxalmente, mais arriscado, reside nas técnicas de aprendizado profundo (*deep learning*), que utilizam *redes neurais artificiais* para reproduzir computacionalmente alguns aspectos do sistema nervoso humano[147]. A arquitetura dessas redes, composta por várias camadas intermediárias ("escondidas"), interpreta padrões invisíveis aos seres humanos e requer matemática complexa[148]. É justamente nessa complexidade operacional que a crítica jurídica e ética se aprofunda.

A primeira e mais notória problemática técnica que desafia o Direito é a *opacidade algorítmica*, frequentemente denominada "caixa-preta" (*black box*)[149]. Um sistema de IA é considerado opaco quando seus processos de tomada de decisão e lógica subjacente são difíceis de entender ou explicar. Em modelos fundacionais, como aqueles usados pela IA Generativa (IA Gen), essa opacidade é intrínseca à própria técnica, que pode envolver 10n parâmetros. Nem mesmo os experts humanos, por vezes, são capazes de explicar um resultado específico[150].

Essa falta de explicabilidade (*explainability*), crucial para criar confiança nos sistemas de IA, mina a capacidade dos indivíduos afetados de contestar uma decisão, o que é um direito fundamental[151]. Como bem advertem as Orientações Éticas para uma IA de Confiança, a explicabilidade é necessária para contestar devidamente uma decisão, apresentar dados adicionais para a sua modificação ou excluir dados relevantes[152].

O segundo ponto, e o mais diretamente ligado à temática da discriminação, é que a *Inteligência Artificial não é neutra, nem subjetiva*[153]. Ela é, invariavelmente, uma criação humana, e a *subjetividade humana está presente em todas as etapas* do seu desenvolvimento e

[144] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 143.
[145] *REVISTA JURÍDICA DA PRESIDÊNCIA*. Brasília, DF: Centro de Estudos Jurídicos da Presidência, v. 27, n. 142, mai/ago. 2025. p. 147.
[146] SAYAD, 2023, p. 26.
[147] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 288.
[148] SAYAD, 2023, p. 81.
[149] *Ibid.*
[150] REVISTA JURÍDICA DA PRESIDÊNCIA, ref. 136, p. 238.
[151] Ibid., p. 239.
[152] Ibid.
[153] SAYAD, 2023, p. 18.

uso[154]. Os vieses inerentes à sociedade são transportados para a tecnologia por meio da *base de dados de treinamento*, que, se for incompleta, insuficiente ou historicamente tendenciosa, produzirá resultados e predições igualmente enviesados[155]. A pesquisadora Dora Kaufman, uma referência central neste campo, sugere que, dada a natureza multidisciplinar da IA, é crucial que as equipes de desenvolvedores sejam *diversificadas*, agregando profissionais das Ciências Exatas e das Ciências Humanas, justamente para incorporar o olhar ético e crítico desde a concepção do sistema[156].

A *discriminação algorítmica* surge, portanto, como a reprodução e, por vezes, a amplificação, de vieses sociais preexistentes, como os de raça e gênero, quando o algoritmo baseia seu raciocínio na apreciação de características perceptíveis acerca de uma pessoa[157]. A mineração de dados sem cautela pode reproduzir padrões existentes de discriminação ou herdar preconceitos de tomadores de decisão prévios[158]. A crítica social é tão severa que Cathy O'Neil (2020) classifica os algoritmos como possíveis "*armas de destruição matemáticas*" (ADMs), justamente porque, ao serem baseados em escolhas humanas falíveis, causam impactos sociais extremamente nocivos, especialmente a *discriminação de populações mais vulneráveis*[159].

Um exemplo prático e de alta relevância jurídica no contexto brasileiro é o uso da *Tecnologia de Reconhecimento Facial* (TRF). Esta tecnologia de IA trata dados biométricos, expressamente definidos no Art. 5º, II, da LGPD como dados sensíveis. O tratamento indevido ou irregular de tais informações tem o potencial de *ocasionar ou ampliar contextos discriminatórios*[160]. O *racismo algorítmico* no reconhecimento facial ocorre, em grande parte, devido à falta de treinamento adequado da máquina para reconhecer com acurácia faces negras ou femininas, sendo a acurácia para homens brancos, em muitos casos, inversamente proporcional à de mulheres negras[161].

Como já adiantado, o Art. 6º, IX, da LGPD estabelece o *Princípio da Não Discriminação*, vedando o tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos. Além disso, a lei concede ao titular de dados o direito de *solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado* de dados pessoais que afetem seus interesses, como o perfilamento (Art. 20, *caput*)[162].

---

[154] SAYAD, 2023, p. 27.
[155] *Ibid.*, p. 76.
[156] KAUFMAN, 2022, p. 15.
[157] REVISTA JURÍDICA DA PRESIDÊNCIA, ref. 136, p. 57.
[158] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 39.
[159] O'NEIL, 2020. p. 7.
[160] COSTA; KREMER, 2022, p. 2.
[161] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 289.
[162] COSTA; KREMER, 2022, p. 17.

No entanto, há uma crítica jurídica veemente sobre a efetividade desse mecanismo. O Art. 20, § 1º, da LGPD permite que o controlador se resguarde, fornecendo informações sobre o tratamento "*observados os segredos comercial e industrial*"[163]. Essa ressalva, ao proteger o segredo de negócio da empresa, impõe um obstáculo substancial ao direito à explicabilidade e, consequentemente, à capacidade do titular de contestar o resultado, especialmente quando o sistema opera como uma *black box*[164]. Se a transparência for obstruída, a opacidade algorítmica prevalece, remetendo a uma opacidade típica de sistemas não regulados[165].

Ademais, os desafios regulatórios se agravaram com a ascensão da IA Gen, cuja tecnologia constitutiva, como as *Redes Adversariais Generativas* (GAN), utiliza duas redes neurais em oposição (*uma gera, outra avalia*), otimizando a precisão na correspondência com os dados de treinamento[166]. Embora a IA Gen prometa otimização no setor público e no Judiciário, ela introduz *riscos operacionais* e sistêmicos, incluindo a *imprecisão nos resultados* e a *alucinação* (falha em encontrar uma solução, gerando respostas fictícias)[167].

No Judiciário brasileiro, já se verificou o risco de decisões judiciais baseadas em *jurisprudências falsas* geradas por IA Gen. Tais falhas ameaçam a segurança jurídica e o devido processo legal[168]. Diante disso, a *Corregedoria Regional da Justiça Federal da 1ª Região* (Circular COGER 33/2023) recomendou cautela e reforçou a necessidade de *supervisão e divulgação responsável* do uso da IA na elaboração de decisões judiciais, especialmente quanto ao uso de ferramentas generativas não homologadas[169].

Em termos de tipologia de riscos, o funcionamento dos sistemas de IA Gen no Judiciário se confronta com riscos operacionais, como a *baixa explicabilidade* e a perda de autonomia decisória do operador do Direito[170]. A ideia mais básica da explicabilidade é que utilizadores de IA tenham acesso a explicações a respeito de seus resultados, o que é uma medida de transparência essencial para a *black box*[171].

O *Projeto de Lei nº 2338/2023*, que visa instituir o Marco Legal da IA no Brasil, estrutura-se, em seus primeiros artigos, em fundamentos axiológicos, prevendo expressamente a *igualdade, a não discriminação, a transparência e a explicabilidade*[172]. Contudo, a crítica

---

[163] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 238.
[164] *Ibid.*
[165] COSTA; KREMER, 2022, p. 17.
[166] KAUFMAN, 2022, p. 214.
[167] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 155.
[168] *Ibid*.
[169] *Ibid.* p. 157.
[170] *Ibid.* p. 245.
[171] *Ibid.* p. 239.
[172] *Ibid.* p. 158.

construtiva aponta que, embora o projeto se preocupe com vieses discriminatórios no banco de dados, ele demonstra uma atenção desproporcional à *governança* e aos *vieses discriminatórios* em detrimento de garantir, materialmente, o direito ao trabalho e a educação em face desta tecnologia[173].

Para além da regulação brasileira, as experiências internacionais, como o *Regulamento de Inteligência Artificial* (RIA) da União Europeia, aprovado em junho de 2024, reforçam a necessidade de um *enfoque rigoroso e baseado em princípios*, classificando os sistemas de IA em níveis de risco (*alto, médio e baixo*) para aplicar requisitos proporcionais, com forte ênfase na proteção de direitos fundamentais, incluindo a não discriminação. Essa abordagem europeia, segundo a doutrina, busca um equilíbrio entre a proteção dos direitos e a promoção da inovação tecnológica[174].

Diante do potencial discriminatório dos sistemas baseados em IA, a solução jurídica não pode ser apenas reativa (*ex post*), mas deve ser fundamentalmente *preventiva*[175]. A estratégia de "Ética por Design" (*Ethics by Design*) é sugerida como imperativa, exigindo que a preocupação ética e a antevisão de possíveis consequências sociais sejam garantidas desde o início do processo de projeção e desenvolvimento dos sistemas de IA[176]. Isso implica integrar a *participação humana nos processos decisórios* de sistemas de IA, garantindo que as pessoas não estejam sujeitas a decisões tomadas unicamente por mecanismos automatizados[177].

Afinal, a responsabilidade e a prestação de contas (*accountability*) continuam sendo humanas. A IA, por mais sofisticada que seja, é uma *máquina sintática, não semântica*. Ela computa informações, mas não possui a capacidade de *argumentar,* de ter *consciência* ou ter *autonomia*, atributos essenciais para a manifestação de conduta[178]. O discurso que confere à IA uma aparência lúdica e inocente, ou que a humaniza com verbos como "*decidir*" ou "*deliberar*", corre o risco de naturalizar a exclusão de responsabilidade civil de quem a utiliza, por meio da alegação de "*fortuito*"[179]. Contudo, o ordenamento jurídico brasileiro já possui repertório normativo, como a *responsabilidade objetiva* para atividades de risco (Art. 927, Parágrafo Único, do Código Civil) e o *Código de Defesa do Consumidor* (CDC), aptos a endereçar os

[173] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 160.
[174] *Ibid*. p. 23.
[175] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 132.
[176] KELLER, 2022, p. 72-73.
[177] COSTA; KREMER, 2022, p. 17.
[178] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 74.
[179] *Ibid.,* p. 83.

danos decorrentes do uso da IA, especialmente quando envolve a proteção de dados sensíveis, onde o risco de falha é inerente à natureza da atividade[180].

A proteção dos direitos fundamentais, como a dignidade e a não discriminação, exige a criação de regulações que garantam *a transparência, a equidade e a possibilidade de revisão* das decisões tomadas por IA[181]. A discussão, que se iniciou com o questionamento sobre a capacidade de raciocínio das máquinas, hoje se consolida na crítica sobre a *justiça do algoritmo e a justiça do design*[182], clamando por uma *filosofia algorítmica* e uma hermenêutica comprometida com o contexto sociojurídico, de modo a garantir que a IA beneficie a sociedade como um todo, sem reproduzir o *colonialismo de dados* ou exacerbar as desigualdades[183].

3.2. Casos concretos evidenciando discriminação algorítmica

Ao criar uma alta tecnologia capaz de simular o intelecto humano e otimizar tarefas com uma rapidez e eficiência superiores, a IA trouxe consigo alguns riscos jurídicos e sociais de contornos dramáticos: a *discriminação algorítmica*[184]. Este fenômeno, que surge como um desdobramento da discriminação estrutural presente nas sociedades humanas, ganha um poder de multiplicação e opacidade nos algoritmos inteligentes que são treinados com dados históricos enviesados[185]. Em vez de neutralidade, a IA tem replicado e amplificado preconceitos de raça, gênero e classe[186], levando a consequências lesivas em diversas esferas, desde o mercado de trabalho até o sistema de justiça criminal, e até mesmo na dinâmica da democracia.

A replicação de vícios sociais por sistemas automatizados não é um fenômeno totalmente novo. Já em 1988, a Comissão para Igualdade Racial do governo britânico expôs a discriminação de negros e mulheres no processo de seleção para a *Escola de Medicina de St. George's Hospital*[187]. O sistema computacional que realizava a triagem, treinado por humanos, concedia avaliações menos favoráveis a mulheres e minorias étnicas, reproduzindo a crença comum de que as carreiras femininas seriam interrompidas pelos deveres maternos, e pontuando negativamente pessoas com certos locais de nascimento ou sobrenomes[188]. Este caso é um

---

[180] PINHEIRO, 2021, p. 161.
[181] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 63.
[182] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 4.
[183] SAYAD, 2023, p. 136.
[184] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 60.
[185] *Ibid.,* p. 17.
[186] *Ibid.,* p. 57.
[187] WEDY, Gabriel; HUPFFER, Haide Maria; WEYERMÜLLER , André Rafael. *Direito e inteligência artificial: perspectivas para um futuro ecologicamente sustentável* [recurso eletrônico]. – São Leopoldo: Casa Leiria, 2024, p. 38-39.
[188] *Ibid.*

precursor fundamental, demonstrando que, mesmo antes da sofisticação do *deep learning* (DL), a tecnologia servia como vetor para a discriminação humana[189].

O advento do *machine learning* permitiu que os algoritmos gerassem conhecimento por meio da extração de padrões de grandes bases de dados, ou seja, "*aprendessem*" sem receber instruções explícitas[190]. Essa capacidade, embora revolucionária, é altamente suscetível aos vícios contidos em sua matéria-prima. O caso emblemático que chocou o mercado de tecnologia ocorreu entre 2014 e 2018 com a *Amazon.com*[191].

A *Amazon* desenvolveu um sistema de IA para automatizar a revisão de currículos de potenciais empregados. Desta forma, o algoritmo foi treinado com os registros de contratações de uma década, período em que havia uma esmagadora predominância de homens na indústria de tecnologia[192]. Consequentemente, o *software* ensinou a si mesmo que candidatos do sexo masculino eram preferíveis, penalizando currículos que continham a palavra "feminino" (como em "capitã do clube de xadrez feminino") e rebaixando graduadas de faculdades exclusivas para mulheres[193]. O sistema reproduziu, assim, um viés de gênero, desconsiderando currículos de mulheres de forma sistemática. Tal episódio ilustra a discriminação algorítmica por *erro estatístico* ou por *enviesamento não intencional* associado à inadequação dos dados de treinamento (*training data*)[194].

A manifestação mais perturbadora da discriminação algorítmica ocorre no sistema de justiça. Em 2016, a agência jornalística investigativa *ProPublica* divulgou o relatório "*Machine Bias*", questionando a acurácia do *software* COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), usado em tribunais dos EUA para prever o risco de reincidência criminal[195]. O estudo concluiu que o sistema atribuía aos réus afro-americanos a classificação de "*alto risco*" quase o dobro de vezes em comparação com réus brancos[196]. Embora o sistema não utilizasse características raciais explicitamente, ele se valia de *proxies* (como prisões anteriores do detento ou de seus familiares) que se mostravam mais impactantes sobre a população negra, reforçando a seletividade penal estrutural[197]. Essa é uma manifestação

[189] WEDY; HUPFFER; WEYERMÜLLER, 2024, p. 38-39.
[190] KAUFMAN, 2022, p. 12.
[191] WEDY; HUPFFER; WEYERMÜLLER, 2024, p. 39.
[192] *Ibid.*
[193] SAYAD, 2023, p. 78.
[194] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1298-1299.
[195] KAUFMAN, 2022, p. 197.
[196] *Ibid.*
[197] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1301-1302.

clássica de discriminação indireta, onde o modelo estatisticamente irretocável, mas latente, comporta prejuízos a classes sistematicamente excluídas[198].

Paralelamente, o ano de 2016 viu emergir o mais emblemático caso de manipulação comportamental massiva e discriminação política: o escândalo envolvendo a *Cambridge Analytica (CA)* e o *Facebook*, detalhado com profundidade por Brittany Kaiser em seu livro *Manipulados*[199]. O objetivo da CA, segundo o ex-CEO Alexander Nix, era o "*direcionamento microcomportamental*" com base na personalidade dos eleitores, construindo modelos preditivos altamente eficazes. A CA valeu-se do *superávit* comportamental, ou seja, dados profundos e percepções que permitiam novas possibilidades de manipulação[200].

A empresa chegou a possuir "*mais de 5 mil data points sobre 230 milhões de adultos estadunidenses*". Esses dados, em grande parte, foram obtidos de maneira ilícita por meio do infame *Friends API* do *Facebook*, que permitiu a coleta de informações privadas de milhões de usuários e seus amigos sem o consentimento da maioria. A negligência do *Facebook* e a total falta de supervisão do governo federal sobre dados pessoais permitiram que os objetivos da *Cambridge* se concretizassem[201].

A influência da CA transcendeu o mero convencimento; ela se dedicou à supressão de eleitores (*deterrence*), uma tática intrinsecamente discriminatória e ilegal nos EUA. Brittany Kaiser confirma que, durante o balanço da campanha de Donald Trump em 2016, foram identificados grupos-alvo chamados "*deterrence*", visando a supressão de eleitores[202]. Materiais ofensivos, como vídeos fora de contexto ("*Superpredadores*"), foram usados para incitar ódio racial e pressionar uma minoria a *não votar* em Hillary Clinton, com alvo específico em eleitores afro-americanos em áreas vulneráveis, como o *Little Haiti*, em Miami, e a zona rural da *Geórgia.* Kaiser afirma que o *software* da CA permitiu a distribuição de mensagens de forma tão eficiente, que os eleitores chegavam a agir contra seus próprios interesses de longo prazo[203].

O sucesso da estratégia foi argumentado por Shoshana Zuboff com base na queda de 7% no comparecimento de eleitores negros comparativamente a 2012[204]. No entanto, autores como Yochai Benkler, Robert Faris e Hal Roberts, após análise exaustiva, ponderaram que é "*altamente improvável*" que a publicidade psicograficamente microdirecionada da CA tenha

---

[198] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1301-1302.
[199] KAISER, Brittany. *Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque*. São Paulo: HarperCollins, 2020.
[200] ZUBOFF, 2021. p. 337-338.
[201] KAISER, 2020, p. 416.
[202] *Ibid.*, p. 304.
[203] *Ibid.*, p. 315.
[204] KAUFMAN, 2022, p. 263.

sido o fator decisivo, atribuindo a polarização a problemas institucionais e ao ecossistema de mídia, mas reconhecendo que a CA utilizou a hipersegmentação do Facebook como qualquer cliente pagante[205]. Independentemente do grau de influência nas urnas, a CA demonstrou como algoritmos de perfilamento de personalidade, alimentados por *Big Data*, podem ser transformados em armas para minar direitos fundamentais, como o direito ao voto e o direito à não-discriminação[206].

A rápida ascensão das tecnologias de reconhecimento facial e biométrico revelou novos e alarmantes vieses. Já em 2010, notou-se o problema nas câmeras *Nikon*, que frequentemente interpretavam que pessoas de origem asiática estavam de olhos fechados, levantando o debate sobre viés tecnológico racista[207]. O erro decorria da imprecisão na medição da distância entre os olhos, fruto de um aprendizado fragmentado da máquina, possivelmente pela escassez de imagens de pessoas asiáticas no conjunto de dados de treinamento[208]. Similarmente, o *Google* foi compelido a corrigir seu algoritmo "*racista*" após falhas em suas ferramentas de reconhecimento de imagens identificarem pessoas negras como gorilas[209].

A pesquisa acadêmica trouxe a comprovação científica desses vieses. O estudo "*Gender Shades*" (2018), conduzido por Joy Buolamwini e Timnit Gebru, apurou resultados discriminatórios com viés de gênero e raça em algoritmos de análise facial[210]. Buolamwini, protagonista do documentário *Coded Bias*, descobriu que o sistema de reconhecimento facial que ela pretendia usar em um projeto só a reconhecia quando ela colocava uma máscara branca[211].

O relatório do *Instituto Nacional de Padrões e Tecnologia* (NIST) nos EUA, em 2019, evidenciou que as maiores taxas de precisão dos softwares de reconhecimento facial eram encontradas entre homens brancos de meia-idade, enquanto asiáticos e afro-americanos eram identificados com erro até 100 vezes mais[212]. Tal demonstração de viés racial e de gênero pressionou as gigantes de tecnologia, levando *IBM, Microsoft e Amazon* a anunciarem, em junho de 2020, a limitação do uso de seus sistemas de reconhecimento facial pelos departamentos de polícia[213].

---

[205] KAUFMAN, 2022, p. 263.
[206] ZUBOFF, 2021. p. 338.
[207] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1299-1300.
[208] *Ibid.*
[209] *Ibid.*, p. 1287.
[210] KAUFMAN, 2022, p. 197.
[211] LIMA; SABOYA, 2022, p. 251.
[212] KAUFMAN, 2022, p. 97.
[213] *Ibid.*

No setor de serviços e finanças, a discriminação também se manifesta de maneira sutil. Em 2019, o *Apple Card*, cartão de crédito lançado pela Apple em parceria com o Goldman Sachs, foi acusado de discriminação contra mulheres. Denúncias apontaram que o algoritmo oferecia limites de crédito consideravelmente menores para clientes do gênero feminino em comparação com os masculinos, mesmo para casais com perfis financeiros idênticos. Este caso se enquadra na discriminação pelo uso de informações sensíveis ou na limitação do exercício de um direito[214].

Outro caso notório foi o do *Twitter* que, ao final de 2020, admitiu a falha em um algoritmo de reconhecimento facial responsável pelo *cropping* (enquadramento) automático de imagens. Usuários relataram que, em fotos com uma pessoa negra e uma branca, a tendência algorítmica era manter a pessoa branca no enquadramento ideal, resultando na exclusão da pessoa negra[215].

A aplicação da IA na segurança pública no Brasil tem gerado um cenário de vulnerabilidade exacerbada, onde a seletividade penal ganha uma aparência de objetividade algorítmica. As TRFs têm sido o carro-chefe de grandes promessas de segurança pública, mas têm resultado na *prisão por engano de inocentes*, majoritariamente homens negros[216]. Casos concretos no Brasil, como a detenção de uma mulher em Copacabana em 2019 por erro do sistema, e a prisão injusta do cientista de dados *Raoni Lázaro Barbosa* em 2021, acusado de integrar uma milícia, demonstram os graves riscos[217].

Em dezembro de 2021, o pedreiro José Domingos Leitão foi acordado pela polícia em sua casa no Piauí, a mais de mil quilômetros do local do crime, após um programa de reconhecimento facial confundi-lo com um criminoso procurado em Brasília[218]. Em todos esses casos, o elemento comum era serem homens negros, confirmando que a TRF tem sido uma ferramenta de reprodução e potencialização de opressões já existentes na sociedade, uma vez que as máquinas carregam as percepções racistas de seus produtores e dos dados que as alimentam[219], aplicando aqui a teoria de O'Neil sobre as ADMs.

A regulação dessa dinâmica exige uma resposta jurídica robusta e alinhada aos direitos humanos, especialmente o direito à não-discriminação, que na perspectiva da Corte Interamericana de Direitos Humanos (Corte IDH) alcança o status de *jus cogens*. A Corte IDH

[214] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1295.
[215] *Ibid*., p. 1292-1293.
[216] COSTA; KREMER, 2022, p. 150-151.
[217] *Ibid.*
[218] *Ibid*.
[219] *Ibid*., p. 149.

veda qualquer distinção de tratamento com finalidade arbitrária e impõe aos Estados a obrigação de adotar medidas compensatórias para grupos historicamente em desvantagem[220].

Diante da discriminação algorítmica, deve ser exigido um especial dever de justificação por parte dos programadores e das empresas na utilização de dados de pessoas que componham grupos vulneráveis, sob pena de o algoritmo ser presumidamente discriminatório[221].

3.3. Impactos éticos e jurídicos

A alta complexidade inerente aos processamentos, que podem envolver parâmetros, resulta na dificuldade de explicabilidade (*black-box*), fragilizando a prestação de contas dos agentes de tratamento[222].

A pesquisadora Dora Kaufman alerta que a base de dados para o treinamento de algoritmos de IA, pois a "*base de dados para treinar algoritmo de IA não é salsicha*"[223], e a complexidade e opacidade dos sistemas favorecem a especulação, sendo que a explicabilidade não é um princípio novo, mas que conflita com o próprio funcionamento das redes neurais[224]. Essa lacuna compromete a efetividade do direito do titular previsto na LGPD, de acessar "*informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada*" (art. 20, § 1º)[225]. O RIA da UE, por sua vez, busca justamente esse equilíbrio, exigindo que os provedores de sistemas de IA mantenham documentação técnica detalhada para garantir a *rastreabilidade das decisões automatizadas*[226]. A inabilidade em garantir a transparência do processo decisório é agravada quando a IA Gen é empregada em setores sensíveis.

No âmbito do Poder Judiciário, por exemplo, o uso dessas ferramentas, que por vezes são treinadas em conjuntos de dados amplos e inespecíficos[227], tem gerado o fenômeno da "alucinação" (*delírio*), onde a IA não consegue encontrar respostas no banco de dados e produz resultados falsos de forma convincente. Um caso ilustrativo de 2023, envolvendo um juiz federal que utilizou o *ChatGPT* para fundamentar uma decisão com jurisprudência fictícia, demonstra como tais incidentes ameaçam a segurança jurídica e o devido processo legal,

[220] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 145, p. 407.
[221] KAUFMAN, 2022, p. 111.
[222] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 238.
[223] KAUFMAN, 2022. p. 39.
[224] *Ibid*., p. 258.
[225] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 238
[226] *Ibid*., p. 26.
[227] *Ibid.,* p. 258.

violando o art. 11 do CPC referente ao dever de fundamentação do juiz[228]. Essa tecnologia, por não possuir semântica ou consciência, delega a tomada de decisão a um raciocínio puramente estatístico[229].

O Legislativo brasileiro responde a essa complexa realidade por meio de um esforço de *atualização sistêmica* do ordenamento jurídico, demonstrado pela reforma do Código Civil (CC) e pela proposição de novos marcos regulatórios. O Anteprojeto de Reforma e Atualização do CC, entregue ao Senado Federal em abril de 2024 e convertido em PL 4/2025[230], reconhece que o texto anterior, proveniente de um projeto iniciado nos anos 1970, "*já nasceu velho*"[231], e não está adequado à "*digitalização da vida*"[232]. A reforma não propõe um novo código, mas uma atualização, sendo a inclusão do capítulo sobre o Direito Civil Digital uma iniciativa de vanguarda[233]. Este novo livro é estruturado em dez capítulos, abordando temas cruciais como a IA, o patrimônio digital, e a identidade de crianças e adolescentes no ambiente virtual[234]. A finalidade dessa inclusão é harmonizar o Direito com a era digital, promovendo maior segurança jurídica[235].

No cerne dessa atualização, o Anteprojeto define os *neurodireitos* como parte dos direitos da personalidade, os quais, em consonância com o Art. 11 do CC, são *intransmissíveis*, *irrenunciáveis* e *insuscetíveis de limitação voluntária*[236]. As categorias sugeridas incluem: liberdade cognitiva, privacidade mental, integridade mental, e *proteção contra vieses discriminatórios*[237]. Esta iniciativa alinha-se a movimentos internacionais e à PEC nº 29/2023, que busca a inclusão da proteção à *integridade mental* e à *transparência algorítmica* entre os direitos fundamentais[238]. Tais direitos fundamentais, que já possuem proteção constitucional pela via interpretativa, seriam significativamente reforçados por esta positivação[239].

No contexto do Direito Digital, a visão doutrinária de Patrícia Peck Pinheiro enfatiza a necessidade de um arcabouço normativo que harmonize a inovação com a proteção dos direitos humanos. Em sua análise, a "*abertura e colaboração*" devem ser fundamentos essenciais, como

---

[228] *Ibid*., p. 247.
[229] REVISTA JURÍDICA DA PRESIDÊNCIA, ref. 136, p. 141.
[230] PACHECO, Rodrigo (org.). *A reforma do Código Civil*: artigos sobre a atualização da Lei nº 10.406/2002. Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2025.p. 17.
[231] *Ibid*., p. 71.
[232] *Ibid*., p. 410.
[233] *Ibid*., *op. cit*.
[234] *Ibid*., p. 390.
[235] *Ibid*., p. 388.
[236] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 214.
[237] *Ibid*., *op. cit.*
[238] PACHECO, 2025. p. 401.
[239] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 213.

preconizado no Marco Civil da Internet, atuando o Direito Digital como um paradigma para uma nova era[240].

Ainda que a LGPD tenha fornecido a primeira base, ela se revelou *insuficiente textualmente e estruturalmente* em face da volatilidade tecnológica[241]. Uma falha grave reside na omissão do veto presidencial ao Art. 20 (que tratava da intervenção humana nas decisões automatizadas), vetado por razões utilitárias e econômicas[242]. Esta lacuna contraria o disposto no Art. 22.3 do GDPR europeu e, ao não garantir o direito à intervenção humana e à contestação, pode conduzir a um *déficе de proteção* dos direitos do paciente lesado[243].

Um avanço regulatório específico para a proteção de grupos vulneráveis no ambiente digital materializou-se com a Lei nº 15.211, de 17 de setembro de 2025, denominada *Estatuto Digital da Criança e do Adolescente* (*Lei Felca*). Esta lei estabelece normas de proteção para crianças e adolescentes em ambientes digitais, aplicando-se a todo produto ou serviço de tecnologia da informação que lhes seja direcionado ou de provável acesso no País[244]. O diploma impõe ao controlador de dados, especialmente no tratamento para fins não estritamente necessários à operação do produto ou serviço, a obrigação de *mapear e mitigar riscos*, e de elaborar um *Relatório de Impacto*, *Monitoramento* e *Avaliação da Proteção de Dados Pessoais*, que deve ser compartilhado sob requisição da autoridade administrativa autônoma de proteção dos direitos de crianças e adolescentes no ambiente digital. Em uma medida de transparência e dever de informar, a Lei exige que as embalagens de equipamentos eletrônicos com acesso à internet comercializados no Brasil contenham um adesivo que informe os pais sobre a necessidade de proteger os menores de conteúdo inadequado[245].

Quanto à *discriminação algorítmica* e seus desafios, o fenômeno é reconhecido como a evolução de um problema estrutural social, que é exacerbado no paradigma da sociedade da informação[246]. O desenvolvimento de algoritmos a partir do estabelecimento de estereótipos de pessoas reais exige, sob a perspectiva dos standards protetivos internacionais, um *dever de*

---

[240] PINHEIRO, 2021, p. 332.
[241] PACHECO, 2025. p. 388.
[242] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 336.
[243] *Ibid.*
[244] BRASIL. Lei nº 15.211, de 17 de setembro de 2025. *Estabelece normas de proteção para crianças e adolescentes em ambientes digitais e altera a Lei nº 13.709, de 14 de agosto de 2018* (Lei Geral de Proteção de Dados Pessoais). [S.l.: s.n.], 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm
[245] *Ibid.*
[246] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 145, p. 400.

controle estatal sobre os estereótipos utilizados durante o processo de programação algorítmica, visando a exclusão de todos os estereótipos negativos[247].

Os *desafios regulatórios* são particularmente críticos no *setor da Saúde*, onde a IA (como em sistemas de diagnóstico médico) é uma fonte de grande progresso, mas também coloca em risco direitos fundamentais, como a privacidade e a não discriminação[248]. A IA pode otimizar a eficácia das políticas públicas na saúde e a personalização de serviços, mas seu avanço rápido levanta questões éticas e legais significativas[249]. O PL nº 2.338/2023, que busca regular a IA no Brasil, propõe a regulamentação baseada no *nível de risco*, impondo mais responsabilidades em situações de maior impacto nos direitos ou na saúde[250].

A natureza sensível dos dados tratados (informações biométricas, genéticas e de saúde) demanda um nível elevado de proteção. A falta de um equilíbrio regulatório pode comprometer a confiança entre pacientes e profissionais[251]. Para mitigar esses riscos, é crucial o uso de métodos adequados de desidentificação e fortalecimento da privacidade para a reutilização de registros médicos no treinamento de sistemas de IA. Além disso, inovações como a IA podem, inadvertidamente, incentivar a solicitação de exames não clinicamente relevantes apenas para otimizar os sistemas de IA, comprometendo a privacidade médica[252].

Para enfrentar essas questões, há a proposição de criação de uma *Lei Federal sobre Segurança Cibernética na Saúde* (*LSCS*), que complementaria a LGPD, focando na proteção robusta de dados sensíveis na telemedicina e no uso de IA, exigindo medidas técnicas obrigatórias como criptografia avançada e órgãos fiscalizadores dedicados [253] . A regulamentação para a incorporação da IA na saúde está em fase inicial, concentrando-se em recomendações, mas espera-se uma adoção mais ágil da tecnologia e o consequente fortalecimento das normas jurídicas para aumentar a responsabilização por violações[254].

---

[247] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 145, p. 410.
[248] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 24.
[249] *Ibid*., *op. cit.*
[250] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 145, p. 425.
[251] *Ibid.,* p. 433.
[252] *Ibid.,* p. 425.
[253] VECCHIO, Fabrizio Bon. *Direito médico digita*l / Fabrizio Bon Vecchio, Ricardo Souto, Thélio Farias. – Leme/SP: AM2, 2025. p. 175-179.
[254] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 145, p. 438.

4. COMPATIBILIDADE ENTRE A LGPD E A TECNOLOGIA

4.1. Análise crítica das disposições legais

Rememora-se que a incursão do Direito na regulação da esfera digital manifesta-se como um imperativo constitucional inadiável e, não se trata de frear o progresso da tecnologia, mas de assegurar que a inovação seja intrinsecamente compatível com os direitos fundamentais da pessoa natural, assegurado pela Constituição Federal e demais Leis Federais, especialmente à *autodeterminação informativa* e a *não discriminação*, que se veem ameaçados pela *opacidade algorítmica* e pelo poder concentrado das grandes plataformas. A jornada regulatória brasileira, mesmo que ainda seja um embrião no ordenamento jurídico, ainda não possuí a rigidez necessária para enfrentar os riscos sistêmicos da IA.

Manifestamente, o ponto de partida histórico dessa compatibilidade forçada é o Marco Civil da Internet, estruturado com um caráter eminentemente principiológico, reafirma os valores constitucionais como a liberdade de expressão e a proteção da privacidade (Art. 3º, II e III)[255]. Contudo, a análise crítica revela que, ao tentar proteger a liberdade de expressão e impedir a censura, o legislador incorreu em uma omissão parcial ao regular de forma insuficiente a proteção dos internautas[256]. Mesmo após 10 anos em vigor, o cerne da controvérsia ainda reside no Art. 19 do MCI, que instituiu o modelo do judicial *notice and take down*, condicionando a responsabilização civil dos provedores de aplicações por danos decorrentes de conteúdo gerado por terceiros à inércia após uma *ordem judicial específica* para remoção[257].

Logo, a insuficiência do MCI frente à economia de dados preparou o terreno para a promulgação da LGPD, que se consolidou como um marco regulatório de aplicação *transversal*. A LGPD objetiva harmonizar o avanço tecnológico e econômico com a proteção dos direitos humanos, o livre desenvolvimento da personalidade e a dignidade[258].

Considerando ainda que o ordenamento jurídico brasileiro não possui arcabouço legal sobre a temática, à compatibilidade entre a LGPD e a tecnologia se faz necessária, pois as disposições legais demonstram uma consciência dos riscos da IA, mas carregam ambiguidades cruciais que demandam análise crítica aprofundada.

---

[255] MARQUES; MARTINS; MARTINS, 2024, p. 57.
[256] *Ibid.,* p. 130.
[257] *Ibid.,* p. 298.
[258] LIMA; SABOYA, 2022, p. 275.

Em primeiro lugar, o tratamento da *Anonimização* (Art. 5º, III e XI; Art. 12) é central. O legislador definiu o dado anonimizado como aquele que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento[259]. A anonimização é, na sua fase inicial, uma operação de tratamento de dado pessoal, o que significa que o dado original submetido ao processo deve ser, antes de tudo, objeto de legítimo tratamento. Criticamente, isso impede que a anonimização, *per se*, legalize uma atividade de tratamento que já era ilícita por falta de base normativa[260].

O ponto mais sensível é o reconhecimento, no Art. 12, da *reversibilidade* do processo, mesmo com "*esforços razoáveis*" de terceiros. O consenso científico, validado por estudos como os de Latanya Sweeney, e de Arvind Narayanan e Vitaly Shmatikov, rompeu com a "suposição da anonimização robusta" (*robust anonymisation assumption*)[261]. Devido ao enorme volume de dados auxiliares e ao avanço dos algoritmos de reidentificação, reconhece-se que *sempre haverá fatores de risco* de reidentificação. Portanto, a LGPD adota implicitamente um *modelo baseado em riscos* à identificabilidade, onde a avaliação da razoabilidade deve levar em conta fatores objetivos, como custo, tempo, tecnologias disponíveis e a licitude dos meios[262]. A anonimização é, assim, uma ferramenta essencial para cumprir o *princípio da necessidade* (Art. 6º, III), limitando o tratamento ao mínimo indispensável[263].

Em segundo lugar, a LGPD enfrenta a *opacidade algorítmica* e o risco de *discriminação* através da regulação das decisões automatizadas (Art. 20). O Art. 20 assegura ao titular o direito de solicitar a *revisão* das decisões tomadas unicamente por tratamento automatizado[264]. Além disso, o controlador deve fornecer "*informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados*". No entanto, esta disposição foi criticamente fragilizada pela exclusão, via veto presidencial, da expressão "*pessoa natural*"[265]. O veto, justificado por "razões utilitárias e econômicas," contradiz o Art. 22.3 do GDPR e a defesa de intervenção humana obrigatória em casos de alto risco, como no caso da ferramenta de recrutamento da *Amazon* que mostrava viés contra mulheres.

Ainda no Art. 20, a ressalva que protege os segredos comercial e industrial é vista como um obstáculo à transparência efetiva e à explicabilidade, dada a natureza "*black-box*" dos

[259] BRASIL, ANPD, ref. 5, p. 17.
[260] *Ibid*., p. 9.
[261] MACHADO; DONEDA, ref. 101, p. 4.
[262] BRASIL, ANPD, ref. 5, p. 20.
[263] *Ibid*., p. 10.
[264] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 61.
[265] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 336.

modelos de *deep learning*[266]. Essa ressalva dá margem à interpretação de que o sigilo dos algoritmos de IA seria um direito absoluto, ao invés de ser objeto de *ponderação inafastável* diante da colisão com o direito à não discriminação e o direito à explicação. Sem uma explicação compreensível, o direito à revisão de decisões automatizadas torna-se uma mera formalidade[267].

A urgência em regular as externalidades negativas da IA culminou na *Emenda Constitucional nº 115/2022*, que elevou a proteção de dados pessoais ao patamar de direito e garantia fundamental. Essa constitucionalização oferece uma base axiológica robusta para a interpretação de todas as disposições legais e regulamentares[268].

Simultaneamente, o debate em torno do PL nº 2338/2023 reforça a necessidade de uma abordagem *baseada em risco*, similar à adotada no Art. 12 da LGPD, para sistemas de IA de alto ou moderado potencial lesivo. Setores como a saúde, que utilizam IA para diagnóstico e tratamento de dados sensíveis, são classificados como de alto risco[269]. Essa abordagem, alinhada com o GDPR, exige a adoção do PbD, que impõe a proteção dos direitos fundamentais seja um objetivo central e um "*requisito de viabilidade*" desde a concepção do sistema[270].

A jurisprudência e os projetos de lei futuros (como o PL 2338) caminham no sentido de tornar obrigatória a intervenção humana e a realização de *due diligence* para avaliar aspectos discriminatórios em aplicações de IA que afetem grupos vulneráveis[271]. A ANPD, por sua vez, está trabalhando na fixação do entendimento e na elaboração de futuras orientações de cunho técnico e computacional, reconhecendo que a gestão do risco de reidentificação deve ser um processo contínuo e iterativo[272].

Estamos diante, portanto, de uma fase de tolerância e omissão parcial (MCI) para uma fase de regulação principiológica e baseada em riscos (LGPD e propostas de IA), reconhecendo que a compatibilidade entre a tecnologia e os direitos humanos não é automática, mas sim um produto da *interpretação sistemática* e da *ponderação* entre valores em colisão, como a liberdade de expressão e a dignidade da pessoa humana[273].

A exigência de transparência e o reconhecimento dos riscos sistêmicos da IA e dos dados sensíveis demandam que os profissionais do Direito abandonem a visão burocrática e assumam

---

[266] CANTARINI, Paola. *Contribuições ao Projeto de Lei 21/20 - Marco Legal da Inteligência Artificial no Brasil: uma análise inclusiva cosmoética e democrática.* Revista Jurídica da Faculdade de Direito do UniCuritiba (RIMA), [s.d.], p. 18.
[267] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 61.
[268] PACHECO, 2025. p. 391.
[269] WEDY; HUPFFER; WEYERMÜLLER, 2024, p. 190.
[270] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 242.
[271] *Ibid.*, p. 336.
[272] BRASIL, ANPD, ref. 5, p. 18.
[273] CANTARINI, [s.d.], p. 8.

o papel de estrategistas na construção de um ambiente digital ético e justo, sob pena de verem a sociedade buscar "fazer justiça com o próprio mouse"[274]. A tarefa de construir essa ponte regulatória está longe de ser concluída, exigindo o aprofundamento constante da análise crítica das disposições legais diante das disrupções contínuas.

4.2. Vulnerabilidades na fiscalização do uso de dados anonimizados

Como já antecipado, a *compatibilidade entre o diploma de proteção de dados e a tecnologia* – mormente no que concerne às operações que envolvem sistemas complexos e o processamento de grandes volumes de informações – é balizada por uma tensão estrutural que se exacerba nas *vulnerabilidades inerentes à fiscalização do uso de dados ditos anonimizados*.

A gênese desse panorama remonta à instauração da disciplina legal para o uso da Internet no país com a vigência do MCI que estabeleceu o primeiro feixe de princípios e garantias, incluindo a proteção da privacidade[275]. Contudo, o regime de responsabilidade civil adotado, notadamente em seu Art. 19, ao exigir prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização do provedor de aplicações por atos ilícitos de terceiros, se revelou insuficiente e excessivamente favorável às grandes empresas de tecnologia[276].

Essa escolha legislativa, influenciada por modelos internacionais como a Section 230 do *Communications Decency Act* (CDA) dos EUA (1996), acabou por cristalizar um modelo de *irresponsabilidade* que transfere o ônus da solução dos conflitos (como *cyberbullying* e desinformação) ao indivíduo ofendido, forçando-o a buscar uma via judicial morosa, enquanto o conteúdo ofensivo se propaga à velocidade da luz[277]. Em paralelo à insuficiência do regime de responsabilização, a expansão do *fenômeno da plataformização* (o aumento significativo na prestação de serviços online) e a onipresença da coleta de informações evidenciaram o nascimento de uma nova forma de *vulnerabilidade digital do usuário*[278]. A sociedade passou a ser classificada por meio de perfis virtuais automatizados, descrevem como a transição da *condição humana para a condição informática*[279].

---

[274] PINHEIRO, 2021, p. 336.
[275] MARQUES; MARTINS; MARTINS, 2024, p. 298.
[276] *Ibid.*
[277] *Ibid.,* p. 303.
[278] *Ibid.,* p. 149.
[279] *Ibid.,* p. 147.

A urgência dessa adequação normativa foi drasticamente exposta pelas revelações do caso de *Edward Snowden*[280]. A figura do "*homem de vidro*"[281], o cidadão cujas informações são monitoradas e registradas independentemente de consulta posterior, consolidou a percepção de que a tecnologia, quando não balizada, ameaça à liberdade, a igualdade, a autonomia e a democracia[282]. O dado, que se tornou *mais valioso que o petróleo*[283], demandou uma legislação que enfrentasse o novo panorama de assimetria de poder e a *vulnerabilidade digital* dos usuários[284].

A despeito da ampla proteção conferida às informações pessoais pela LGPD e, de forma especialíssima, aos *dados sensíveis*, o arcabouço normativo brasileiro introduziu um conceito que, em face da acelerada capacidade técnica, revela uma *vulnerabilidade estrutural na fiscalização*: o *das informações desidentificadas* (dados anonimizados)[285].

A LGPD define a informação desidentificada como aquela que se refere a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de sua operação. O Art. 12 dessa legislação, consagra o que se pode classificar como a "*ilusão da anonimização*" ou a *cláusula de reversibilidade*: a aplicação das regras de proteção se torna novamente cabível a um determinado conjunto de informações se a *reversão da desidentificação for viável ou acabar por ocorrer*. Esse dispositivo transfere o ônus da prova para o agente que utiliza a informação, mas expõe uma falha de compliance legal, uma vez que a capacidade de reidentificação por meio de técnicas de cruzamento de "*big data*" avança mais rapidamente do que os métodos de desidentificação.

A incerteza quanto à validade do procedimento de anonimização exige cautela extrema na formulação das bases legais que dão suporte à operação com informações. A dependência excessiva no consentimento, por exemplo, pode resultar em "*fadiga do consumidor*" e apatia[286], sendo o consentimento, muitas vezes, invalidado por ser composto por textos abstratos, longos e de difícil compreensão, o que coloca o titular em situação de vulnerabilidade. Em um ambiente onde o *compartilhamento massificado de dados pessoais* contribui para o vício de validade do consentimento[287], a fiscalização da irreversibilidade da desidentificação torna-se um exercício quase quimérico.

---

[280] LIMA, Marcelo Chiavassa de Mello Paula; ANDRADE, Vitor Morais de. *Manual de direito digital* / Prefácio Marcelo Gomes Sodré. - 2.ed. - São Paulo: Tirant lo Blanch, 2023., 352 p., p. 285.
[281] *Ibid.,* p. 283.
[282] MARQUES; MARTINS; MARTINS, 2024, p. 51.
[283] LIMA; ANDRADE, 2023, p. 285.
[284] MARQUES; MARTINS; MARTINS, 2024, p. 298.
[285] *Ibid.,* p. 196.
[286] LIMA; ANDRADE, 2023, p. 206.
[287] *Ibid.,* p. 215.

A fragilidade da fiscalização da desidentificação é inseparável do risco de *discriminação algorítmica*. A legislação nacional de proteção estabelece a não discriminação como princípio basilar, proibindo a operação de informações para *fins discriminatórios*[288]. Este vetor se conecta diretamente à proteção dos dados pessoais sensíveis, cujo rol é restrito, abarcando elementos como *origem racial ou étnica, convicção religiosa, dados referentes à saúde ou à vida sexual, e dados genéticos ou biométricos*[289].

A jurisprudência demonstrou a seriedade da violação a esse rol restrito em *outubro de 2020*, quando o Ministro Edson Fachin, no julgamento da ADI 6.561, considerou inconstitucional uma lei estadual de Tocantins que criava um *Cadastro Estadual de Usuários Dependentes de Drogas*. O Ministro argumentou que a lei violava o Art. 2º, II e IV da legislação nacional de proteção, por envolver *dados sensíveis relacionados à saúde* sem prever formas de controle prévio, comunicação ou consentimento, configurando violação da autodeterminação informativa. Esse debate, que também permeia a criação de bancos de dados genéticos[290], demonstra que a vulnerabilidade dos titulares perante sistemas de classificação e categorização é uma preocupação constitucional ativa.

O dilema da discriminação se projeta de forma aguda nos sistemas de pontuação de crédito (*Credit Score*) e nos modelos de Sistema Financeiro Aberto (*Open Banking*), que se tornou uma realidade no Brasil com inúmeros benefícios ao titular[291]. Os modelos que fornecem o score de crédito levantam a questão da *auditabilidade*: "É possível auditá-las? Como saber se estão ou não viciadas?"[292].

Com efeito, a legislação nacional de proteção garante ao titular o direito de solicitar a *revisão das decisões tomadas unicamente com base em processamento automatizado de informações pessoais*[293]. Mais do que isso, o Art. 20, § 1º, da referida legislação impõe ao controlador o dever de fornecer *informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada*[294]. Caso a negativa seja fundamentada em *segredo comercial ou industrial*, o Art. 20, § 2º, prevê a possibilidade de a agência nacional de fiscalização realizar *auditoria no algoritmo*, justamente para verificar a eventual discriminação[295]. Essa disposição é um mecanismo crucial para enfrentar as quatro espécies de

[288] LIMA; ANDRADE, 2023, p. 206.
[289] *Ibid.*, p. 215.
[290] *Ibid.*, p. 216.
[291] *Ibid.*, p. 245.
[292] *Ibid.*, p. 228.
[293] *Ibid.*, p. 218.
[294] *Ibid.*, p. 228.
[295] *Ibid.*

discriminação algorítmica classificadas pela doutrina: por erro estatístico, por generalização, pelo uso de informações sensíveis, ou por limitação do exercício de direitos[296].

O campo da responsabilidade civil das plataformas (provedores de aplicações) por conteúdo gerado por terceiros, regido pelo Art. 19 do MCI, revelou-se o epicentro da incompatibilidade normativa. O modelo adotado, o judicial *notice and take down*, estabelece que a responsabilidade civil do provedor só se configura se, após ordem judicial específica, ele permanecer inerte na remoção do conteúdo infrator[297].

Essa regra, concebida sob o paradigma da neutralidade, mostrou-se falha diante do fenômeno da *plataformização da vida humana*, em que as plataformas deixaram de ser meras transmissoras de conteúdo para se tornarem *verdadeiros reguladores do discurso público*[298], atuando como *network gatekeepers*.

O Art. 19 do MCI entrou em crise não apenas pela sua ineficácia na proteção de direitos, mas pela sua insuficiência no combate à *desinformação* (*fakenews*) e ao *vazamento de dados*, fenômenos que se avolumaram após 2014[299]. A desinformação, frequentemente impulsionada por *contas inautênticas* (perfis falsos ou robôs), e a ocorrência de *vazamento de dados massivos* levaram a uma reinterpretação crítica da imunidade do provedor. A doutrina e a jurisprudência passaram a questionar se o modelo de responsabilidade mitigada assegura impunidade, diante da assimetria de meio, que é dominada por robôs e algoritmos[300].

A tentativa política de reverter essa tendência crítica, notadamente a *Medida Provisória nº 1.068/2021*, que tentou restringir o poder das redes sociais de moderarem conteúdos, foi prontamente barrada e declarada inconstitucional. O STF suspendeu sua eficácia, reforçando que a MP violava conquistas constitucionais consagradas[301].

A partir de *2023*, o debate sobre a constitucionalidade do Art. 19 alcançou o Plenário do Supremo Tribunal Federal, nos Recursos Extraordinários 1.037.396 (*Tema 987*) e 1.057.258 (*Tema 533*). Os votos dos Ministros refletiram a convicção de que há uma *omissão legislativa parcial* e que o Art. 19 deve ser reinterpretado à luz da realidade tecnológica[302].

---

[296] MARQUES; MARTINS; MARTINS, 2024, p. 74-75.
[297] *Ibid.*, p. 298.
[298] *STF: redes respondem por posts mesmo sem ordem judicial; veja tese*. In: MIGALHAS. [S. l.], 27 jun. 2025. Disponível em: https://www.migalhas.com.br/quentes/433462/stf-redes-respondem-por-posts-mesmo-sem-ordem-judicial-veja-tese.
[299] MARQUES; MARTINS; MARTINS, 2024, p. 220.
[300] *Ibid.*, p. 310-311.
[301] *Ibid.*, p. 212-213.
[302] *STF: redes respondem por posts mesmo sem ordem judicial; veja tese*. In: MIGALHAS. [S. l.], 27 jun. 2025. Disponível em: https://www.migalhas.com.br/quentes/433462/stf-redes-respondem-por-posts-mesmo-sem-ordem-judicial-veja-tese.

O voto do Ministro Dias Toffoli (Relator do *Tema 987*, julgado suspenso em *dezembro de 2024*), por exemplo, defendeu *a inconstitucionalidade parcial e progressiva do Art. 19* e propôs um novo regime de responsabilização[303]. O Relator sugeriu que a responsabilidade civil do provedor de aplicações deveria ser *objetiva e independente de notificação* nos casos em que as plataformas:

> *1. Recomendem, impulsionem (remunerada ou não) ou moderem ativamente conteúdos.*
> *2. Lidem com contas inautênticas ("perfil falso") ou contas desidentificadas/automatizadas (chatbots ou robôs).*
> *3. Permitam a veiculação de ilícitos graves, como crimes contra o Estado Democrático de Direito e terrorismo.*

Nesse cenário de insegurança jurídica, a ANPD, por sua vez, tem participado ativamente no debate público, defendendo o equilíbrio entre a proteção dos direitos e a inovação tecnológica[304].

O Poder Judiciário, ante a iminente regulação da tecnologia em seu próprio âmbito, demonstrou a consciência das falhas na fiscalização de dados. Embora as diretrizes iniciais viessem da Resolução CNJ nº 332/2020, a necessidade de adequação à LGPD é constante. A regulação futura no âmbito do Judiciário, conforme as diretrizes examinadas nos excertos (usando a referência temporal da Resolução CNJ 615/2025 para o contexto de IA generativa e proteção de dados), estabelece mecanismos explícitos para mitigar a vulnerabilidade do anonimato e a opacidade dos sistemas automatizados[305].

Essas diretrizes impõem que:

> *1. Os modelos de IA sejam desenvolvidos sob os paradigmas de privacy by design (preservação da privacidade desde a concepção) e privacy by default (utilização, por padrão, de alto nível de confidencialidade de dados).*
> *2. Os dados utilizados para o treinamento dos sistemas devem ser anonimizados sempre que possível, sendo essa providência obrigatória para dados sigilosos ou protegidos por segredo de justiça.*

Crucialmente, para combater a reversibilidade da desidentificação e as falhas na fiscalização, a regulação judicial estabelece a necessidade de *anonimização* ou *pseudoanonimização* na origem. O Art. 29, § 1º, conceitua essa técnica como o processo de

---

[303] *STF: redes respondem por posts mesmo sem ordem judicial; veja tese*. In: MIGALHAS. [S. l.], 27 jun. 2025. Disponível em: https://www.migalhas.com.br/quentes/433462/stf-redes-respondem-por-posts-mesmo-sem-ordem-judicial-veja-tese.

[304] MARQUES; MARTINS; MARTINS, 2024, p. 62.

[305] BRASIL. Conselho Nacional de Justiça. *Resolução n. 615, de 11 de março de 2025. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário*. Diário da Justiça Eletrônico: DJe/CNJ, Brasília, DF, n. 54, p. 2-17, 14 mar. 2025. Disponível em: https://atos.cnj.jus.br/atos/detalhar/6001.

eliminação da identificabilidade antes que os dados sejam transmitidos ou processados pela solução[306].

Ademais, a regulação judicial reforça os instrumentos de transparência e responsabilização já previstos na legislação nacional de proteção, determinando a auditabilidade das soluções, a realização de *monitoramento contínuo* e a *vedação do uso* de sistemas de natureza privada ou externa ao Judiciário para processar dados sigilosos, *salvo quando devidamente anonimizados na origem*[307].

Ao exigir que os sistemas ofereçam documentação atualizada e que os tribunais garantam a segurança dos dados fornecidos por meio de *criptografia robusta*, a jurisdição reconhece que a fiscalização não pode ser passiva[308]. O Judiciário se posiciona como um dos agentes que, através da fiscalização ativa e da imposição de padrões técnicos elevados, tenta compensar as falhas do regime original do MCI e as vulnerabilidades inerentes à reversibilidade da desidentificação. A própria existência do direito de o titular solicitar a revisão de decisões automatizadas, com a possibilidade de auditoria pelo órgão de fiscalização[309], configura uma metodologia de controle *ex post* indispensável à regulação humanitária do campo digital.

O debate, portanto, não se encerra na mera constatação da fragilidade da desidentificação técnica, mas se complexifica na tentativa do sistema jurídico em criar "*soberania*" sobre a técnica. A constante atualização da legislação e a atuação multissetorial da jurisdição, do legislativo e do executivo, são a única resposta possível à natureza volátil e onipresente das tecnologias que seguem transformando a realidade em tempo real.

[306] BRASIL. CNJ. Resolução n. 615. 2025.
[307] *Ibid.*
[308] *Ibid.*
[309] LIMA; ANDRADE, 2023, p. 228.

5. DIRETRIZES PARA MITIGAÇÃO DE RISCOS

5.1. Propostas para aprimoramento regulatório

O primeiro pilar para a mitigação de riscos reside na maturação do ambiente regulatório, exigindo que as estruturas de governança e fiscalização se adaptem à natureza disruptiva dos sistemas algorítmicos[310]. Essa discussão remonta, inclusive, a documentos anteriores à própria LGPD.

Já em *abril de 2014*, o Parecer 05/2014 do Grupo de Trabalho do Artigo 29º (GT29), órgão consultivo da União Europeia, estabeleceu que a *anonimização de dados* possui um *fator de risco inerente*[311], e que a avaliação da identificabilidade deve considerar o conjunto de meios que poderiam ser "razoavelmente" utilizados por terceiros para reverter o processo. Esse entendimento, ao introduzir uma análise de risco[312], pavimentou o caminho para uma regulação menos binária.

Com a consolidação dos sistemas de IA, a necessidade de controle preventivo ganhou contornos mais firmes. Em *agosto de 2020*, o CNJ promulgou a Resolução nº 332, que regula o uso de ferramentas no Poder Judiciário. Este normativo, reconhecendo os riscos, determinava que, *se vieses discriminatórios tivessem sido identificados antes da produção do software*, eles deveriam ser corrigidos ou o sistema deveria ser *descontinuado*, com a obrigatoriedade de elaboração de um relatório explicativo da decisão[313].

No âmbito internacional, a Comissão Europeia, em *abril de 2021*, apresentou a Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas sobre a IA (*AI Act*)[314]. Esta proposta adota uma abordagem de *risquificação,* exigindo que os sistemas classificados como de "*alto risco*" (especialmente em setores sensíveis como educação e saúde) sejam *previamente auditados por agências reguladoras*, com especial atenção à integridade e vieses das bases de dados[315]. Dora Kaufman ressalta essa necessidade, visto que as tecnologias de *machine learning* e *deep learning* que aprendem por si mesmas colocam novos desafios éticos e a premência de estabelecer arcabouços legais[316].

---

[310] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 69.
[311] MACHADO; DONEDA, ref. 101, p. 13.
[312] BRASIL. ANPD, 2023, ref. 5, p. 17.
[313] LIMA; ANDRADE, 2023, p. 274.
[314] KAUFMAN, 2022, p. 140.
[315] *Ibid.,* p. 41.
[316] *Ibid.,* p. 72.

No cenário brasileiro, a LGPD, embora fundamental, é criticada por se qualificar, majoritariamente, como *repressiva*, atuando posteriormente à ocorrência do dano, em um contexto que clama por *ações de natureza preventiva*[317]. France Netto e Ehrhardt Júnior (2022) argumentam que a insuficiência da tutela se manifesta no Art. 20 da LGPD, que trata da revisão das decisões automatizadas. O Art. 20, que faculta ao titular a solicitação de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, é um mecanismo essencial[318].

Contudo, Paola Cantarini (2023) critica veementemente o fato de a LGPD *não prever a obrigatoriedade da revisão humana* em casos de alto e moderado risco, contrariando o modelo do GDPR (Art. 22.3). Essa lacuna decorre do veto presidencial da expressão "pessoa natural" no Art. 20 da LGPD, motivado por razões utilitárias e econômicas, que não são as mais apropriadas para a tutela de direitos fundamentais[319]. Cantarini defende que o PL sobre IA deve prever o direito de revisão e contestação dos resultados de decisões automatizadas, sendo *obrigatória a intervenção humana* em casos de alto risco e risco moderado[320].

Outra crítica central ao arcabouço normativo brasileiro, com reflexos no aprimoramento regulatório, concerne à proteção do *segredo industrial* e do *sigilo dos algoritmos*. O receio das empresas em expor o funcionamento interno de seus *softwares*, sob alegação de desvantagens mercadológicas, entra em conflito com o direito à transparência e à explicabilidade[321]. A LGPD permite uma interpretação que confere ao *sigilo de algoritmos um caráter quase absoluto*, ao invés de pautar-se na inafastável *ponderação* com direitos fundamentais[322]. Wolfgang Hoffmann-Riem (2022) sugere que a proteção judicial das pessoas afetadas pela opacidade algorítmica poderia ser viabilizada pela introdução de *procedimentos sigilosos nos tribunais*, obrigando as empresas a revelar os algoritmos e seus critérios ao juízo, em especial em casos de ameaça à liberdade[323].

No que tange à fiscalização, a ANPD é vista como a *agência-chave* para garantir a consistência regulatória e a inovação responsável. A Agência, na sua Análise Preliminar do PL 2338/2023[324], confirmou seu papel de guardiã da privacidade e demonstrou a intenção de

[317] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1312.
[318] Ibid., p. 36.
[319] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 336.
[320] *Ibid.*
[321] *REVISTA JURÍDICA DA PRESIDÊNCIA*, ref. 136, p. 60.
[322] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 339.
[323] *Ibid.,* p. 340.
[324] MARQUES; MARTINS; MARTINS, 2024, p. 63.

fortalecer suas atribuições para promover auditorias e fiscalizar os potenciais riscos de dados tratados por sistemas de IA[325].

Propõe-se, ainda, a adoção de um procedimento de *due diligence algorítmico*[326]. Cantarini (2023) argumenta que tal procedimento deve ser propiciado para *avaliar os aspectos discriminatórios* no uso de dados sensíveis ou de grupos vulneráveis (como idosos, crianças, adolescentes, enfermos). Esse procedimento deve ser realizado desde o início do *desenvolvimento da tecnologia* (*protection by design*)[327], visando identificar e mitigar potenciais resultados discriminatórios.

No mesmo sentido, a Resolução nº 615 do CNJ (2025), ao tratar da IA Gen, exige a *curadoria dos dados* usados no desenvolvimento, priorizando fontes seguras, rastreáveis e auditáveis, além de exigir monitoramento contínuo para a prevenção e mitigação de vieses discriminatórios ilegais ou abusivos[328].

5.2. Propostas legislativas para fortalecer a proteção contra discriminação

A necessidade de fortalecer o sistema antidiscriminatório passa pela correção das omissões e ambiguidades nas normas atuais, em especial no MCI, LGPD, e nos projetos de lei em tramitação.

O MCI é alvo de severas críticas por sua insuficiência. O instrumento normativo, após uma década de vigência, mostrou-se *anacrônico*, operando sob uma crença equivocada de que as normas do CDC não se aplicariam às relações na internet. A falta de diálogo entre o MCI e o CDC prejudicou a proteção da *vulnerabilidade digital*, notadamente dos consumidores[329].

Um ponto crítico é a *responsabilidade civil pela moderação de conteúdo por IA*. Luiz Carlos Goiabeira Rosa (2022) argumenta que o MCI falhou em tratar aprofundadamente essa questão, perdendo uma oportunidade ímpar de regular a responsabilidade civil atinente ao *ciclo de vida da IA*, à definição dos agentes e à caracterização de risco[330]. O MCI estabeleceu um sistema de responsabilidade para provedores (Art. 19) que não se mostrou apto a proteger os usuários contra os danos causados por algoritmos opacos[331]. Ademais, o MCI não abordou a responsabilização do provedor pela adoção incorreta da IA, que pode remover conteúdo de

[325] BRASIL. ANPD, ref. 45, p. 7.
[326] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 335-336.
[327] *Ibid.,* p. 339.
[328] BRASIL. CNJ. Resolução n. 615. 2025.
[329] MARQUES; MARTINS; MARTINS, 2024, p. 130.
[330] *Ibid.,* p. 258-262.
[331] *Ibid.,* p. 195.

forma autônoma e imprecisa, falhando em compreender o contexto e o valor social das expressões. O avanço tecnológico exige a *designação de responsabilidades* aos atores que detêm significativo poder de mercado[332].

No âmbito da LGPD, a crítica mais contundente recai sobre o rol de *dados pessoais sensíveis* (Art. 5º, II). O rol expressa preocupação com o potencial discriminatório, vedando o tratamento para fins discriminatórios ilícitos ou abusivos (Art. 6º, IX). No entanto, a lei é omissa quanto à inclusão expressa da *identidade de gênero e da orientação sexual*[333].

Elaine Keller (2022) e Carvalho, Botelho & Trejo (2023) defendem que ambos os elementos *devem ser tratados como dados sensíveis*, devido ao grande potencial de violação de direitos fundamentais e de discriminação que representam para a população LGBTQIA+[334]. A doutrina majoritária propõe a interpretação do rol do Art. 5º, II, como *exemplificativo*, utilizando o *potencial discriminatório* como chave de leitura para configurar o dado como sensível[335].

Keller (2022) questiona a abrangência do termo "vida sexual" na LGPD (Art. 5º, II), argumentando que a identidade de gênero se refere à autoidentificação e ao modo como a pessoa se vê e quer ser vista pela sociedade, e não se confunde com as relações íntimas[336], sendo, portanto, uma lacuna que precisa de alteração legislativa. A ausência de proteção explícita compromete a *segurança jurídica* dos titulares e acentua a marginalização[337]. Costa e Kremer (2022) sugerem que a identidade de gênero seja interpretada como dado sensível por revelar informações que podem gerar discriminação[338].

No que tange aos novos projetos de lei, o *PL nº 2.338/2023*, que regula o uso da IA, tem sido objeto de crítica construtiva. O projeto estabelece o objetivo de promover uma IA *ética e livre de preconceitos* (Art. 5º, I) e garante a transparência dos dados sensíveis (Art. 7º, III), alinhando-se à LGPD. Contudo, a principal crítica reside na falta de clareza sobre o *sistema de responsabilidade civil*. O Art. 6º, VI, que trata da responsabilização e prestação de contas, possibilita uma interpretação de *responsabilidade subjetiva*[339], o que, segundo críticos, tornaria a produção de prova (*probatio diabolica*) excessivamente onerosa para o cidadão sem conhecimento técnico[340].

---

[332] MARQUES; MARTINS; MARTINS, 2024, p. 195.
[333] CARVALHO; BOTELHO; TREJO, 2023, p. 289.
[334] Ibid., p. 275.
[335] Ibid., p. 286.
[336] KELLER, 2022. p. 22.
[337] COSTA; KREMER, 2022, p. 160.
[338] Ibid., p. 159.
[339] Ibid., p. 152.
[340] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 246.

Juliano Maranhão critica a falha em atribuir a responsabilidade objetiva como regra no PL, argumentando que a subjetividade inviabilizaria a inovação e o investimento no país[341]. A tese da responsabilidade objetiva é defendida por muitos, inclusive no Anteprojeto do Código Civil, que se baseia na vulnerabilidade do usuário e no risco da atividade[342]. Diante da opacidade intrínseca de sistemas como o *deep learning*, é urgente adotar uma abordagem de *responsabilidade objetiva* para sistemas de alto risco, como já proposto pelo Parlamento Europeu (Resolução de *outubro de 2020*)[343].

Outra proposta legislativa crucial é a proteção dos *neurodireitos*. A *PEC nº 29/2023* visa incluir a *proteção à integridade mental* e à *transparência algorítmica* entre os direitos e garantias fundamentais, refletindo o risco do aumento progressivo do uso de *neurotecnologias*[344]. Além disso, o PL nº 522/2022 já buscava conceitualizar e regulamentar a proteção dos *dados neurais* na LGPD, reforçando a segurança dos dados. O Anteprojeto de Reforma do Código Civil, apresentado em *abril de 2024*, também abraça a temática, propondo um novo livro sobre Direito Digital e prevendo garantias específicas contra o uso coercitivo de neurotecnologias e a vedação de manipulações da atividade mental[345].

O *Anteprojeto do Código Civil* (2024) busca alinhar o país às tendências globais, estabelecendo um regime de responsabilidade civil adaptado. O texto, ao abordar temas como a responsabilidade das plataformas *online* e o uso de IA, demonstra a necessidade de segurança jurídica[346]. Prevê a *responsabilidade objetiva* em casos de risco especial (Art. 927-B)[347] e a possibilidade de o juiz ser provocado a determinar a adoção de medidas preventivas concretas. Essa abordagem é vista como essencial, dado que a sociedade digital exige uma *ampliação da responsabilização*, exigindo conduta preventiva[348].

Em suma, as propostas legislativas devem integrar os pedidos de banimento de sistemas de alto potencial discriminatório, como o reconhecimento facial biométrico para categorização por etnia ou gênero[349], e a inclusão de mecanismos de ações afirmativas algorítmicas, exigindo a programação dos algoritmos para impedir a discriminação e a avaliação prévia dos dados de treinamento[350].

---

[341] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 247.
[342] *Ibid.,* p. 296.
[343] CANTARINI, [s.d.], p. 5.
[344] PACHECO, 2025. p. 401.
[345] *Ibid.,* p. 403.
[346] *Ibid.,* p. 400.
[347] *Ibid.,* p. 110-111.
[348] PINHEIRO, 2021, p. 308.
[349] LIMA; SABOYA, 2022, p. 392-393.
[350] CANTARINI; GUERRA FILHO; KNOERR. 2022. p. 339.

5.3. Soluções técnicas para evitar reidentificação

O terceiro pilar de mitigação reside na aplicação de soluções técnicas avançadas, partindo do pressuposto crítico de que a *anonimização total é uma falácia*[351].

Desde o ano 2000, os trabalhos de Latanya Sweeney e, posteriormente, de Arvind Narayanan e Vitaly Shmatikov (2007 e 2010), já demonstravam as sérias falhas nas práticas de anonimização tidas como seguras[352]. Esses estudos comprovaram que a *suposição da anonimização robusta* (a ideia de que simples operações de eliminação de atributos garantiam a privacidade) estava quebrada, e que o desenvolvimento dos algoritmos de mineração de dados e o enorme volume de dados auxiliares disponíveis tornam o risco de *reidentificação sempre presente*[353].

Diante disso, a LGPD adota um conceito de anonimização que se baseia nos *esforços razoáveis e disponíveis* (Art. 12), o que, segundo o Estudo Técnico da ANPD (2023), introduz um modelo *baseado em risco* para delimitar o que é dado pessoal. O critério dos esforços razoáveis aponta, na verdade, para a teoria objetiva do conceito amplo de dado pessoal[354].

O Estudo Técnico da ANPD (2023) estabelece que a anonimização deve ser entendida como um *processo contínuo baseado em riscos*, e não apenas como a aplicação isolada de técnicas[355]. Essa abordagem é fundamental porque não é factível considerar que o processo resultará em um cenário de risco zero. A gestão do risco de reidentificação deve ser realizada de forma contínua durante todo o tratamento, com a obrigação de atualizar o nível de risco sempre que houver operações de inclusão, alteração ou deleção de dados[356].

Os riscos de reidentificação são categorizados em três tipos principais, conforme o Parecer 05/2014 do GT29 e o Estudo Técnico da ANPD:

> *1. Distinção (singling out): Possibilidade de isolar registros que destacam um indivíduo em uma base de dados.*
> *2. Possibilidade de ligação (linkability): Capacidade de estabelecer conexão entre dois ou mais registros relativos ao mesmo indivíduo ou grupo.*
> *3. Inferência: Possibilidade de deduzir o valor de um atributo a partir de outros atributos.*

Para mitigar esses riscos, a adoção de técnicas de anonimização e *Tecnologias de Aprimoramento da Privacidade* (PETs) é essencial[357]. O desenvolvimento de sistemas de IA,

---

[351] BRASIL, ANPD, ref. 6, p. 7.
[352] MACHADO; DONEDA, ref. 101, p. 4.
[353] *Ibid.*
[354] BRASIL, ANPD, ref. 5, p. 21.
[355] *Ibid.*, p. 21-22.
[356] BRASIL, ANPD, ref. 6, p. 12.
[357] OYADOMARI; COSTA; RIBEIRO, 2023. p. 19.

conforme a jurisprudência, deve *minimizar o uso de informações sensíveis*, adotando *mecanismos de anonimização e criptografia*[358].

A *pseudonimização* é uma forma de tratamento pela qual o dado perde a associação a um indivíduo, exceto pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro[359]. A ANPD, no contexto do Judiciário (Resolução de março de 2024), determina que o compartilhamento de dados deve ser feito apenas *se anonimizados ou pseudoanonimizados na origem.* Anonimização na origem significa que o processo técnico de eliminação da identificação é realizado *antes* que os dados sejam transmitidos ou processados pela solução de IA[360].

As ferramentas de ofuscação de dados, uma categoria das PETs, incluem a *privacidade diferencial* e *dados sintéticos*, que operam alterando os dados ou adicionando "ruído" para preservar a privacidade, permitindo o aprendizado de máquina[361]. No entanto, as PETs não são uma "solução mágica", pois não resolvem, por exemplo, problemas relacionados a *vieses indevidos* que possam estar refletidos nos dados originais[362].

Finalmente, França Netto e Ehrhardt Júnior (2022) (p. 1309) destacam que as soluções técnicas devem ser complementadas pela capacitação ética e pelo *maior zelo* nas etapas de coleta de dados, treinamento e aperfeiçoamento dos modelos. É fundamental o *desenvolvimento de algoritmos destinados à própria investigação de enviesamentos*[363]. A ideia é buscar uma *proteção sistêmica*, desde a concepção tecnológica (*protection by design* e *security by design*), reconhecendo que a tecnologia deve ser programada para impedir a discriminação. A complexidade e a ineficácia da autorregulamentação reforçam a necessidade de que essas soluções técnicas sejam exigidas e supervisionadas por um quadro normativo vinculativo, como o proposto pelo *AI Act*[364].

[358] CASALI SILVA, 2023. p. 52-53.
[359] MACHADO; DONEDA, ref. 101, p. 4.
[360] BRASIL. CNJ. Resolução n. 615. 2025.
[361] OYADOMARI; COSTA; RIBEIRO, 2023. p. 19-20.
[362] *Ibid.*
[363] FRANÇA NETTO; EHRHARDT JÚNIOR, 2022, p. 1309.
[364] KAUFMAN, 2022, p. 161.

6. CONCLUSÃO

A ascensão inelutável da Inteligência Artificial (IA) no seio da sociedade da informação consolidou a Lei Geral de Proteção de Dados Pessoais (LGPD) como um dique normativo fundamental, ancorado na proteção dos direitos de liberdade, privacidade e o livre desenvolvimento da personalidade.

Contudo, a presente análise demonstrou, que o arcabouço normativo brasileiro, em sua configuração atual, apresenta vulnerabilidades cruciais que demandam aprimoramento inadiável para enfrentar os riscos sistêmicos da discriminação algorítmica, especialmente no trato de dados pessoais sensíveis. Reconhecendo que a anonimização não se configura como um estado binário de risco zero, mas sim como um processo contínuo baseado na gestão de riscos e da reversibilidade, o profissional do Direito deve assumir uma postura de estrategista para impor diretrizes corretivas, de natureza jurídica e técnica, que transcendam a mera observância da lei fria.

Em primeiro e relevante lugar, torna-se imperiosa a correção da lacuna criada pelo *veto presidencial à intervenção humana por "pessoa natural"* no processo de revisão de decisões automatizadas, fragilizando o Art. 20 da LGPD. Essa omissão, justificada por razões utilitárias e econômicas, compromete a efetividade do direito de contestação do titular e contraria o modelo protetivo do GDPR (Art. 22.3).

Para sistemas de IA classificados como de alto ou moderado risco, especialmente naqueles que afetam direitos fundamentais em setores como saúde, justiça e análise de crédito, a *intervenção humana obrigatória* é um pilar fundamental para mitigar riscos e assegurar o exercício da cidadania. Destarte, é inafastável a *revisão legislativa do Art. 20 da LGPD* para determinar a obrigatoriedade da revisão por pessoa natural nas decisões automatizadas que afetem significativamente os interesses dos titulares.

Adicionalmente, dada a complexidade técnica e a opacidade (*black box*) inerente a modelos de *deep learning*, a teoria da responsabilidade civil deve ser adaptada, sendo urgente a adoção da *responsabilidade civil objetiva* como regra para atividades de IA de alto risco, baseada na vulnerabilidade do usuário e no risco intrínseco da atividade, rompendo com a interpretação de responsabilidade subjetiva que tornaria a prova do dano (*probatio diabolica*) excessivamente onerosa para o cidadão comum.

O enfrentamento da opacidade algorítmica exige um regime de *transparência* que não seja mitigado pelo receio de exposição do segredo comercial e industrial. Embora o Art. 20, § 1º, preveja o fornecimento de informações claras sobre os critérios de decisão, a ressalva que

protege o *sigilo comercial* impõe um obstáculo substancial ao direito de explicabilidade (*explainability*).

Essa colisão de direitos deve ser resolvida por meio da *ponderação inafastável*, e não pela prevalência irrestrita do sigilo dos algoritmos. Para tanto, deve ser implementado um *procedimento de due diligence algorítmico*, exigindo auditorias prévias e o monitoramento contínuo dos sistemas para identificar e mitigar vieses discriminatórios nos *datasets* de treinamento e nos modelos, desde a concepção. O controle *ex post* deve ser fortalecido, garantindo a auditabilidade dos sistemas ANPD.

A proteção contra a discriminação algorítmica deve ser estruturada sob o paradigma do *Privacy by Design* (PbD) e *Ethics by Design*, exigindo que a prevenção do dano e a tutela da privacidade sejam requisitos de viabilidade e sejam integrados desde a concepção do sistema. Uma vez que o risco de reidentificação é inerente e dinâmico, desafiando a ilusão da anonimização plena, a aplicação de técnicas de *anonimização ou pseudoanonimização na origem* (*anonymization or pseudoanonymization at the origin*) é fundamental. Essa técnica, que exige a desidentificação antes que os dados sejam transmitidos ou processados pela solução de IA, é crucial para o tratamento de dados sigilosos, conforme diretrizes do CNJ.

Além disso, os agentes de tratamento devem adotar *Tecnologias de Aprimoramento da Privacidade* (PETs), como a privacidade diferencial e dados sintéticos, que operam para preservar a privacidade, permitindo simultaneamente a utilidade dos dados para o machine learning. A anonimização deve ser tratada, inequivocamente, como um processo contínuo baseado em risco, exigindo atualização constante do nível de risco.

Por derradeiro, o arcabouço normativo, embora reconheça a alta potencialidade lesiva dos dados sensíveis, apresenta uma omissão crítica no rol taxativo do Art. 5º, II, da LGPD: a ausência da menção expressa à *identidade de gênero e à orientação sexual*. A doutrina sustenta, *ab initio*, que o cerne do dado especial reside na sua *potencialidade discriminatória* à luz do pano de fundo sócio-histórico e jurídico.

Portanto, enquanto não houver alteração legislativa, o profissional do Direito deve adotar uma *interpretação material* do Art. 5º, II, da LGPD, reconhecendo a identidade de gênero e a orientação sexual como dados sensíveis. Tal desiderato hermenêutico é necessário para coibir processos sociais de exclusão e segregação e garantir o padrão de proteção elevado para a população LGBTQIA+, cujas informações possuem o potencial de gerar grave violação à personalidade e discriminação. A guarda dos direitos fundamentais na era digital exige a contínua busca por um cabal equilíbrio entre todos os interesses em jogo.

REFERÊNCIAS

BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. In: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo (Coords. gerais). Enciclopédia jurídica da PUC-SP. São Paulo: Pontifícia Universidade Católica de São Paulo, 2022. Tomo: Direito Internacional. Coords. de tomo: Cláudio Finkelstein; Clarisse Laupman Ferraz Lima. 1. ed. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais

BRASIL. Agência Nacional de Proteção de Dados. *Estudo técnico sobre anonimização de dados na LGPD: Análise Jurídica*. Brasília, DF: ANPD, 2023. 27 p. Versão 1.0.

BRASIL. Agência Nacional de Proteção de Dados. *Estudo técnico sobre anonimização de dados na LGPD: uma visão de processo baseado em risco e técnicas computacionais*. Brasília, DF: ANPD, 2023. 27 p. Versão 1.0.

BRASIL. Agência Nacional de Proteção de Dados. *Nota técnica n. 19/2023/FIS/CGF/ANPD*. [S.l.]: ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-19-2023-fis-cgf-anpd.pdf.

BRASIL. ANPD. Nota técnica n. 19/2023/FIS/CGF/ANPD. [S.l.]: ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-19-2023-fis-cgf-anpd.pdf.

BRASIL. Conselho Nacional de Justiça. *Resolução n. 615, de 11 de março de 2025. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário*. Diário da Justiça Eletrônico: DJe/CNJ, Brasília, DF, n. 54, p. 2-17, 14 mar. 2025. Disponível em: https://atos.cnj.jus.br/atos/detalhar/6001

BRASIL. *Constituição da República Federativa do Brasil: de 5 de outubro de 1988*. Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. *Estabelece normas de proteção para crianças e adolescentes em ambientes digitais e altera a Lei nº 13.709, de 14 de agosto de 2018* (Lei Geral de Proteção de Dados Pessoais). [S.l.: s.n.], 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm

CANTARINI, Paola. *Contribuições ao Projeto de Lei 21/20 - Marco Legal da Inteligência Artificial no Brasil: uma análise inclusiva cosmoética e democrática.* Revista Jurídica da Faculdade de Direito do UniCuritiba (RIMA), [s.d.].

CANTARINI, Paola; GUERRA FILHO, Willis Santiago; KNOERR, Viviane Coêlho de Séllos. *Direito e Inteligência Artificial: Fundamentos*. Vol. 4 – Por uma filosofia da inteligência artificial. Rio de Janeiro. Editora Lumen Juris. 2022.

CARVALHO, Pedro Augusto Gil de; BOTELHO, Marcos César; TREJO, Jordy Arcadio Ramirez. *Gênero e sexualidade como dados sensíveis na Lei Geral de Proteção de Dados*. Revista Sapiência: Sociedade, Saberes e Práticas Educacionais, [S.l.], p. 274-297, 2023.

CASALI SILVA, Felipe. *Proteção de Dados Pessoais na Era da Inteligência Artificial*. 2023. 74 f. Monografia (MBA em Inteligência Artificial e Big Data) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2023

COSTA, Ramon; KREMER, Bianca. *Inteligência artificial e discriminação*: *desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial*. Direitos Fundamentais & Justiça, Belo Horizonte, ano 16, p. 145-167, out. 2022.

Diretrizes da OCDE para a *Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais*. Disponível em <http://www.oecd.org/sti/ieconomy/15590254.pdf>.

FRANÇA NETTO, Milton Pereira de; EHRHARDT JÚNIOR, Marcos. *Os riscos da discriminação algorítmica na utilização de aplicações de inteligência artificial no cenário brasileiro*. RJLB, Coimbra/Lisboa/São Paulo, ano 8, n. 3, 2022. 1271-1318.

GUIMARÃES, Maria Raquel; PEDRO, Rute Teixeira. *Direito e Inteligência Artificial*. Editora Almedina. Coimbra. out. 2023.

KAISER, Brittany. *Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque*. São Paulo: HarperCollins, 2020.

KAUFMAN, Dora. *Desmistificando a inteligência artificial*. Belo Horizonte: Autêntica, 2022.

KELLER, Elaine Cristine Zordan. *A tutela da identidade de gênero na LGPD: uma análise na perspectiva de dado sensível*. 2022. 90 f. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) – Programa de Pós-Graduação Profissional Stricto Sensu em Direito, Justiça e Desenvolvimento, Instituto Brasiliense de Direito Público (IDP), São Paulo, 2022. p. 46.

LIMA, Ana Paula Canto de; SABOYA. Maria Beatriz. *Ensaios sobre direito digital, privacidade e proteção de dados* [livro eletrônico]. -- 1. ed. Império Jurídico, 2022. Recife, PE.

LIMA, Marcelo Chiavassa de Mello Paula. ANDRADE; Vitor Morais de. *Manual de direito digital* / Prefácio Marcelo Gomes Sodré. - 2.ed. - São Paulo: Tirant lo Blanch, 2023., 352 p.

MACAU. Gabinete Para a Protecção de Dados Pessoais. *Guia para técnicas básicas de anonimização de dados.* [Tradução de: GUIDE TO BASIC DATA ANONYMISATION TECHNIQUES, publicado pela Personal Data Protection Commission of Singapore, 2018]. Macau: GPDP, 2019. 42 p.

MACHADO, Diego; DONEDA, Danilo. *Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no Direito Brasileiro*. Revista de Direito Civil Contemporâneo. vol. 23/2020, p. 95 – 140, abr – jun 2020. DTR\2021\207.

MACHADO, Diego; DONEDA, Danilo. *Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados*. , vol. 1, p. 99-128, dez. 2018.

MARINHO, Letícia Ramos. *Ausência de regulamentação da IA para a proteção de dados pessoais sensíveis de saúde: análise sobre danos aos titulares*. Revista Sapiência: Sociedade, Saberes e Práticas Educacionais, [S.l.], p. 274-297, 2023.

MARQUES, Claudia Lima; MARTINS, Guilherme Magalhães; MARTINS, Fernando Rodrigues (Coord.). *10 anos marco civil da internet: avaliando impactos e desafios* [recurso eletrônico]. Indaiatuba, SP: Editora Foco, 2024. 296 p. ISBN: 978-65-6120-192-6 (Ebook).

O'NEIL, Cathy. *Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia.* Tradução de Rafael Abraham. 1. ed. Santo André, SP: Editora Rua do Sabão, 2020.

OLIVEIRA, Caio César de. *Apagamento, desindexação e esquecimento: a experiência brasileira na Internet. 2020*. 192 f. Dissertação (Mestrado em Direito Civil) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020.

OYADOMARI, Winston; COSTA, Ramon Silva; RIBEIRO, Manuella Maia. *Proteção de dados pessoais: privacidade e confiança no ambiente digital*. Panorama Setorial da Internet, [S.l.]: Cetic.br|NIC.br, ano 15, n. 2, jun. 2023.

PACHECO, Rodrigo (org.). *A reforma do Código Civil*: artigos sobre a atualização da Lei nº 10.406/2002. Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2025.

PINHEIRO, Patricia Peck. *Direito digital* / Patricia Peck Pinheiro. – 7. ed. – São Paulo: Saraiva Educação, 2021. e-book.

REVISTA JURÍDICA DA PRESIDÊNCIA. Brasília, DF: Centro de Estudos Jurídicos da Presidência, v. 27, n. 141, jan./abr. 2025. Dossiê.

REVISTA JURÍDICA DA PRESIDÊNCIA. Brasília, DF: Centro de Estudos Jurídicos da Presidência, v. 27, n. 142, mai/ago. 2025. p. 147.

SAYAD, Alexandre Le Voci. *Inteligência Artificial e Pensamento Crítico: Caminhos para a educação midiática*. 1. ed. São Paulo: Instituto Palavra Aberta. 2023.

STF: redes respondem por posts mesmo sem ordem judicial; veja tese. In: MIGALHAS. [S. l.], 27 jun. 2025. Disponível em: https://www.migalhas.com.br/quentes/433462/stf-redes-respondem-por-posts-mesmo-sem-ordem-judicial-veja-tese.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Bruxelas, L 119, p. 1-88, 4 de maio de 2016.

VECCHIO, Fabrizio Bon. *Direito médico digital* / Fabrizio Bon Vecchio, Ricardo Souto, Thélio Farias. – Leme/SP: AM2, 2025.

WEDY, Gabriel; HUPFFER, Haide Maria; WEYERMÜLLER , André Rafael. *Direito e inteligência artificial: perspectivas para um futuro ecologicamente sustentável* [recurso eletrônico]. – São Leopoldo: Casa Leiria, 2024.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância*. Tradução de Rafael Abraham. 1. ed. Rio de Janeiro: Editora Intrínseca, 2021. p. 271.